

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年 6 月 10 日 (10.06.2004)

PCT

(10) 国際公開番号
WO 2004/049633 A1

(51) 国際特許分類⁷: H04L 12/28, G06F 15/00
(21) 国際出願番号: PCT/JP2003/014634
(22) 国際出願日: 2003 年 11 月 18 日 (18.11.2003)
(25) 国際出願の言語: 日本語
(26) 国際公開の言語: 日本語
(30) 優先権データ:
特願 2002-339080
2002 年 11 月 22 日 (22.11.2002) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP).
(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 本田 康晃 (HONDA, Yasuaki) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内

Tokyo (JP). 吉川 典史 (KIKKAWA, Norifumi) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 五十嵐 卓也 (IGARASHI, Tatsuya) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 小堀 洋一 (KOBORI, Yoichi) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 森田 岳彦 (MORITA, Takehiko) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).

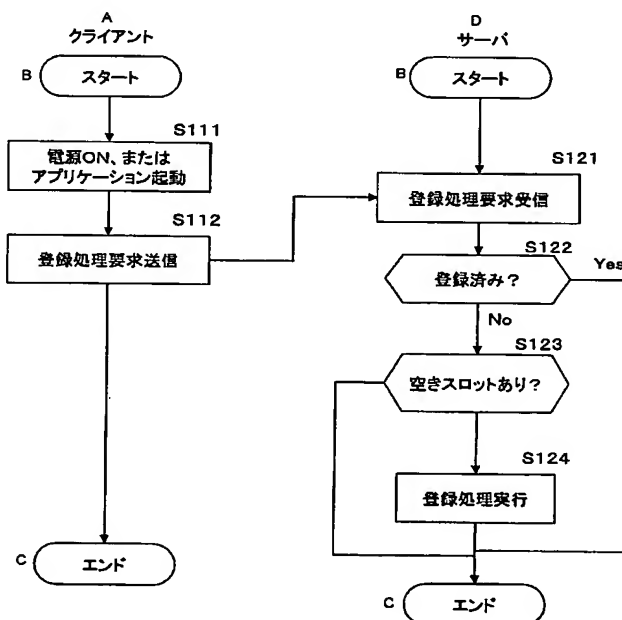
(74) 代理人: 宮田 正昭, 外 (MIYATA, Masaaki et al.); 〒104-0041 東京都中央区新富一丁目 1 番 7 号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo, (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU,

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE, SERVER CLIENT SYSTEM, METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラム



A...CLIENT
B...START
S111...TURN POWER ON OR START APPLICATION
S112...TRANSMIT REGISTRATION PROCESSING REQUEST
C...END
D...SERVER
S121...RECEIVE REGISTRATION PROCESSING REQUEST
S122...REGISTERED?
S123...EMPTY SLOT PRESENT?
S124...EXECUTE REGISTRATION PROCESSING

(57) Abstract: There are provided a device and a method for effectively creating a MAC list as an access control list without causing a load on a user. A registration processing request packet for the MAC list is automatically transmitted by a trigger when a client device connected to a network is turned ON or when a predetermined application such as a service execution application using a home network is started. According to the empty slot condition in the MAC list, a server acquires information such as a MAC address from the reception packet and executes registration processing. With this configuration, it is possible to easily and reliably create a MAC list as an access control list without causing a load on a user.

(57) 要約: アクセス制御リストとしてのMACリストの生成をユーザに負担を強いることなく効率的に生成する装置および方法を提供する。ネットワークに接続されたクライアント機器の電源ON処理、あるいは所定アプリケーション、例えばホームネットワークを利用したサービスの実行アプリケーションを起動する処理のいずれかの処理をトリガとしてMACリストに対する登録処理要求パケットを自動送信する。サーバは、MACリストの空きスロットの状況に応じて、受信パケットからMACアドレス等の情報を取得して登録処理を実行する。本構成により、ユーザの負担を発生させることなくアクセス制御リストとしてのMACリストが容易に確実に生成可能となる。



ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

- (84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告書
- 補正書・説明書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラム

5

技術分野

本発明は、情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、ネットワーク接続された機器間での通信を実行する構成において、ユーザに負担をかけることなく効率的にアクセス権限判定情報を生成し、生成情報に基づくアクセス制限処理を可能とした情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラムに関する。

15 背景技術

昨今のデータ通信ネットワークの普及に伴い、家庭内においても家電機器やコンピュータ、その他の周辺機器をネットワーク接続し、各機器間での通信を可能とした、いわゆるホームネットワークが浸透しつつある。ホームネットワークは、ネットワーク接続機器間で通信を行なうことにより各機器のデータ処理機能を共有したり、機器間でコンテンツの送受信を行なう等、ユーザに利便性・快適性を提供するものであり、今後、ますます普及することが予測される。

このようなホームネットワークの構成に適するプロトコルとしてユニバーサルプラグアンドプレイ（UPnP：Universal Plug and Play）が知られている。ユニバーサルプラグアンドプレイ（UPnP）は、複雑な操作を伴うことなく容易にネットワークを構築することが可能であり、困難な操作や設定を伴うことなくネットワーク接続された機器において各接続機器の提供サービスを受領可能とするものである。また、UPnPはデバイス上のOS（オペレ

ーディングシステム)にも依存せず、容易に機器の追加ができるという利点を持つ。

5 UPnPは、接続機器間で、XML (eXtensible Markup Language) に準拠した定義ファイルを交換し、機器間において相互認識を行なう。UPnPの処理の概要は、以下の通りである。

(1) IPアドレス等の自己のデバイスIDを取得するアドレッシング処理。

10 (2) ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理。

(3) ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理。

15 上記処理手順を行なうことで、ネットワーク接続された機器を適用したサービスの提供および受領が可能となる。ネットワークに新たに接続される機器は、上記のアドレッシング処理によりデバイスIDを取得し、ディスカバリ処理によりネットワーク接続された他のデバイスの情報を取得して、取得情報に基づいて他の機器にサービスの要求が可能となる。

20 しかし、一方、この種のネットワークでは、不正アクセスに対する対策を考慮することも必要となる。ホームネットワーク内の機器、例えばサーバ等には私的なコンテンツや有料コンテンツ等の著作権管理を要求されるコンテンツが格納されることも多い。

25 このようなホームネットワーク内のサーバに格納されたコンテンツは、ネットワーク接続された他の機器からアクセス可能となる。例えば、上述の簡易な機器接続構成であるUPnP接続を実行した機器によってコンテンツを取得することが可能となる。コンテンツが映画データや音楽データの場合、ネットワーク接続機器としてTV、あるいはプレーヤ等を接続すれば、映画を視聴し

たり、音楽を聴いたりすることが可能となる。

コンテンツの利用権を有するユーザの接続した機器によるアクセスは許容されてもよいが、上述のようなネットワーク構成においては、コンテンツ等の
5 利用権を持たないユーザがネットワークに入り込むことも容易である。例えば無線LANによって構成されたネットワークの場合には家の中にあるサーバに対して、戸外、あるいは隣家等から通信機器を利用して不正にネットワークに参入し、コンテンツの搾取を行なうような事態も発生し得る。このような不正なアクセスを許容する構成は、秘密漏洩を生じさせることにもなり、また、
10 コンテンツ著作権の管理の観点からも重要な問題となる。

上述のような不正アクセスを排除するため、例えばサーバにアクセスを許容するクライアントのリストを保持させ、クライアントからサーバに対するアクセス要求の際に、サーバでリストとの照合処理を実行して不正アクセスを排除
15 する構成が提案されている。

例えば、ネットワーク接続機器に固有の物理アドレスであるMAC (Media Access Control) アドレスを、アクセス許容機器リストとして設定するMACアドレスフィルタリングが知られている。MACアドレス
20 フィルタリングとは、ホームネットワーク等の内部ネットワーク(サブネット)と外部ネットワークとを隔離するルータあるいはゲートウェイに、予めアクセスを許容するMACアドレスを登録しておき、受信したパケットのMACアドレスと登録されたMACアドレスとを照合し、登録されていないMACアドレスを有する機器からのアクセスを拒否するものである。なお、この種の技術
25 については、例えば特許文献1(特許公開平10-271154号公報)に開示されている。

しかし、アクセス制限をするためのMACアドレスの登録処理を行なうためには、ネットワークに接続される機器の全てのMACアドレスを調べることが

必要であり、取得した全ての機器のMACアドレス（48bit）をオペレータが入力してリストを作成するという処理が必要となる。このような処理は、例えば特定の会社、団体等、セキュアな環境を構築することが要求される場合には、所定の管理者の下に行なうことも可能であるが、例えば一般家庭に設定
5 されるホームネットワーク環境において、一般ユーザにMACリストの生成、格納を要求することは現実的ではない。

ホームネットワークにおいては、新たな機器の追加処理が行われることは頻繁に発生することであり、このような機器追加処理の際に、ユーザが逐次、機器のMACアドレスを調べて登録処理をしなければならないとすると、ネット
10 ワーク構築の容易性を阻害することになる。

一方、一般家庭においても、PCのみならず、家電機器も含んだネットワーク構成が構築され、どのような機器からでもネットワークにアクセス可能ない
15 わゆるユビキタス環境が構築されつつあり、また、無線LAN等の普及により、通信可能な機器が外部から無線LANに侵入することも容易となっている。このようなネットワーク環境において、ネットワーク接続機器に対する不正アクセスもより発生しやすくなっており、不正なアクセスによる秘密情報の搾取、コンテンツの不正読み取り等が実行される可能性はますます高くなっている。
20 このような状況において、一般ユーザに負担を強いることなく、適切なアクセス制御構成を容易に実現することが求められている。

発明の開示

25 本発明は、上述の問題点に鑑みてなされたものであり、様々な機器がネットワーク接続される構成において、ネットワーク接続機器を有するユーザに負担を強いることなく、容易にかつ的確にアクセス制御構成を構築することを可能とした情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

本発明は、例えば、ネットワーク接続された様々な機器（クライアント）からの処理要求を受信する機器（サーバ）において、クライアント識別により処理要求権限を有するか否かを判断し、処理要求権限のあるクライアントからの要求に対してのみサーバが処理要求に応じる構成を実現し、不正な機器からの処理要求を排除することで秘密漏洩を防止するとともに、コンテンツ著作権についても適正な管理を実現することを可能とした情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

10

本発明の第1の側面は、

アクセス制御リストの生成処理を実行する情報処理装置であり、

アクセス要求機器としてのクライアントからのパケットを受信する受信部と、

15

1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストを格納した記憶部と、

前記受信部における受信パケットに基づくクライアント登録処理に際して、前記MACリストの空きスロットの有無を確認し、空きスロットがある場合にのみ登録可能とする判定を行なう登録可否判定部と、

20

前記登録可否判定部における登録可能の判定に基づいて、前記受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する登録処理部と、

を有することを特徴とする情報処理装置にある。

25

さらに、本発明の情報処理装置の一実施態様において、前記登録処理部は、前記クライアントからの受信パケットのヘッダ部に含まれる送信元MACアドレスを取得し、前記MACリストに対する登録情報として適用する処理を実行する構成であることを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、クライアントからの受信パケットが登録処理要求パケットであるかデータ処理要求であるかを判別するパケット解析部を有し、前記登録可否判定部は、クライアントからの受信パケットが登録処理要求パケットである場合に、

5 前記MACリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、前記登録処理部は、前記登録可否判定部における登録可能の判定に基づく登録処理を実行する構成であることを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置に

10 おいて、前記登録可否判定部は、クライアントからの受信パケットがデータ処理要求パケットである場合に、前記MACリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、前記登録処理部は、前記登録可否判定部における登録可能の判定に基づいて、受信したデータ処理要求パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する

15 登録処理を実行する構成であることを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、前記MACリストの空きスロットの設定処理からの経過時間が予め定められた閾値時間を経過したことを条件として、空きスロットのクローズ処理

20 を実行する制御部を有することを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記登録可否判定部は、クライアントからのデータ処理要求シーケンスが、UPnPプロトコルに従ったシーケンスを確実に実行しているか否かを判定する処理を実行する構成を有し、前記登録処理部は、クライアントからのデータ処理要求シーケンスが、UPnPプロトコルに従ったシーケンスを確実に実行しているとの判定に基づいて、クライアントからの受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する構成である

25 ことを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記登録可否判定部は、クライアントからのデータ処理要求において、UPnPプロトコルに従ったシーケンス中のコンテンツディレクトリサービス(CDS)要求処理が実行されたか否かを判定し、前記登録処理部は、前記コンテンツディレクトリサービス(CDS)要求処理が実行されたとの判定に基づいて、クライアントからの受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する構成であることを特徴とする。

5

10 さらに、本発明の情報処理装置の一実施態様において、前記登録処理部は、クライアントからの受信パケットに格納されたMACアドレスおよびMACアドレスと異なる識別情報を取得し、前記MACリストに対する登録処理を実行する構成であることを特徴とする。

15 さらに、本発明の情報処理装置の一実施態様において、前記MACアドレスと異なる識別情報は、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別情報であることを特徴とする。

さらに、本発明の第2の側面は、

20 ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置であり、

自己のMACアドレスをヘッダ情報中に格納し、前記サーバの保有するMACリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行する制御部を有することを特徴とする情報処理装置にある。

25

さらに、本発明の情報処理装置の一実施態様において、前記制御部は、前記アクセス制御リスト登録処理要求パケットの生成処理において、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別

情報を格納したパケット生成処理を実行する構成であることを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記制御部は、前記アクセス制御リスト登録処理要求パケットをブロードキャスト送信またはマルチキャスト送信として実行する構成であることを特徴とする。

さらに、本発明の第3の側面は、

アクセス要求を受信するサーバと、アクセス要求を実行するクライアントからなるサーバクライアントシステムにおいて、

10 前記クライアントは、

自己のMACアドレスをヘッダ情報中に格納したアクセス制御リスト登録処理要求パケットを、情報処理装置の電源オン処理、または特定アプリケーション起動処理を条件として生成し、送信処理を実行する構成を有し、

前記サーバは、

15 前記クライアントからのアクセス制御リスト登録処理要求パケットを受信し、1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストの空きスロットの有無を確認し、空きスロットがある場合にのみ、前記パケットに基づくクライアント情報の、前記MACリストに対する登録処理を実行する構成を有する、

20 ことを特徴とするサーバクライアントシステムにある。

さらに、本発明のサーバクライアントシステムの一実施態様において、前記サーバは、前記クライアントからの受信パケットのヘッダ部に含まれる送信元MACアドレスを取得し、前記MACリストに対する登録情報として適用する

25 処理を実行する構成であることを特徴とする。

さらに、本発明の第4の側面は、

アクセス制御リストの生成処理を実行する情報処理方法であり、

アクセス要求機器としてのクライアントからのパケットを受信する受信ス

テップと、

1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストの空きスロットの有無を判定する登録可否判定ステップと、

- 5 前記登録可否判定ステップにおける空きスロット有りの判定に基づいて、前記受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する登録処理ステップと、
を有することを特徴とする情報処理方法にある。

- 10 さらに、本発明の情報処理方法の一実施態様において、前記登録処理ステップは、前記クライアントからの受信パケットのヘッダ部に含まれる送信元MACアドレスを取得し、前記MACリストに対する登録情報として適用する処理を実行することを特徴とする。

- 15 さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、クライアントからの受信パケットが登録処理要求パケットであるかデータ処理要求であるかを判別するパケット解析ステップを有し、前記登録可否判定ステップは、前記パケット解析ステップにおける解析結果がクライアントからの受信パケットが登録処理要求パケットであると判定された場合に、前記
20 MACリストの空きスロット有無検出処理に基づく登録可否判定処理を実行することを特徴とする。

- さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法において、前記登録可否判定ステップは、クライアントからの受信パケットがデータ処理要求パケットである場合においても、前記MACリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、前記登録処理部ステップ
25 は、前記登録可否判定部における登録可能の判定に基づいて、受信したデータ処理要求パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行することを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記MACリストの空きスロットの設定処理からの経過時間が予め定められた閾値時間を経過したことを条件として、空きスロットのクローズ処理
5 を実行する制御ステップを有することを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記登録可否判定ステップは、クライアントからのデータ処理要求シーケンスが、UPnPプロト
10 コルに従ったシーケンスを確実に実行しているか否かを判定する処理を実行するステップを含み、前記登録処理ステップは、クライアントからのデータ処理要求シーケンスが、UPnPプロトコルに従ったシーケンスを確実に実行しているとの判定に基づいて、クライアントからの受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理
15 を実行することを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記登録可否判定ステップは、クライアントからのデータ処理要求において、UPnPプロトコルに従ったシーケンス中のコンテンツディレクトリサービス(CDS)要求処理
20 が実行されたか否かを判定するステップを含み、前記登録処理ステップは、前記コンテンツディレクトリサービス(CDS)要求処理が実行されたとの判定に基づいて、クライアントからの受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行することを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記登録処理ステップは、クライアントからの受信パケットに格納されたMACアドレスおよびMACアドレスと異なる識別情報を取得し、前記MACリストに対する登録処理
25 を実行することを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記MACアドレスと異なる識別情報は、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別情報であることを特徴とする。

5 さらに、本発明の第5の側面は、

ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置における情報処理方法であり、

情報処理装置の電源オン処理、または特定アプリケーション起動処理をトリガ情報として検出するトリガ検出ステップと、

10 前記トリガ情報の検出を条件として、自己のMACアドレスをヘッダ情報中に格納し、前記サーバの保有するMACリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行するパケット生成送信処理ステップと、

を有することを特徴とする情報処理方法にある。

15

さらに、本発明の情報処理方法の一実施態様において、前記パケット生成送信処理ステップは、前記アクセス制御リスト登録処理要求パケットの生成処理において、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別情報を格納したパケット生成処理を実行することを
20 特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記パケット生成送信処理ステップは、前記アクセス制御リスト登録処理要求パケットをブロードキャスト送信またはマルチキャスト送信として実行することを特徴とする。

25

さらに、本発明の第6の側面は、

アクセス制御リストの生成処理を実行するコンピュータプログラムであり、

アクセス要求機器としてのクライアントからのパケットを受信する受信ステップと、

1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストの空きスロットの有無を判定する登録可否判定ステップと、

- 5 前記登録可否判定ステップにおける空きスロット有りの判定に基づいて、前記受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する登録処理ステップと、
を有することを特徴とするコンピュータ・プログラムにある。

さらに、本発明の第7の側面は、

- 10 ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置における情報処理方法を実行するコンピュータプログラムであり、

情報処理装置の電源オン処理、または特定アプリケーション起動処理をトリガ情報として検出するトリガ検出ステップと、

- 15 前記トリガ情報の検出を条件として、自己のMACアドレスをヘッダ情報中に格納し、前記サーバの保有するMACリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行するパケット生成送信処理ステップと、
を有することを特徴とするコンピュータ・プログラムにある。

20

本発明の構成によれば、ネットワークに接続されたクライアント機器の電源をONとする処理、あるいは所定アプリケーション、例えばホームネットワークを利用したサービスの実行アプリケーションを起動する処理のいずれかの処理をトリガとして、MACリスト登録処理要求パケットを自動送信し、サーバ側で、MACリストの空きスロットの状況に応じて、受信パケットからMACアドレス等の情報を取得して登録する処理を実行する構成としたので、ユーザの負担を発生させることなくアクセス制御リストとしてのMACリストが容易に、かつ効率的に生成可能となる。

25

また、本発明の構成によれば、サーバにMACリストの空きスロットを設定した後、閾値時間内にクライアントからの登録処理要求パケットを受信しなかった場合には、MACリスト中の空きスロットのクローズ処理を実行する構成としたので、MACリストの空きスロットを放置することがなくなり、サーバが第三者からの登録要求を受信した場合においても登録処理を誤って実行することがなくなり、不正なデータ処理要求に応じることが防止される。

さらに、本発明の構成によれば、クライアントから受信する通常 of データ処理要求に応じてサーバ側で未登録のクライアントを登録する処理を実行する構成としたので、登録処理要求パケットを適用することなくMACリストへのクライアント登録が可能となる。

さらに、本発明の構成によれば、クライアントが、特定のネットワークアクセスコントロール (SNAC) に従ったパケットを送信できない機器であっても、ユニバーサルプラグアンドプレイ (UPnP: Universal Plug and Play) 対応機器であり、UPnPプロトコルに従ったシーケンスを確実に実行している場合には、MACリストへの自動登録が可能となり、ユーザの負担を発生させることのないMACリスト生成が可能となる。

さらに、本発明の構成によれば、MACリストの登録情報としてグローバルユニークな識別子としてのGUIDや、機器に対して設定された固有の鍵情報データを格納し、データ処理要求を受信したサーバが、MACアドレスのみならず、GUIDや鍵情報等の識別データを用いてクライアント確認を実行することが可能となり、高いレベルでのセキュリティ管理が実現される。

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュー

タ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

- 5 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づく、より詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

10 図面の簡単な説明

図 1 は、本発明の適用可能なネットワーク構成例を示す図である。

図 2 は、ネットワーク接続機器の構成例について説明する図である。

図 3 は、サーバの処理機能を説明するブロック図である。

- 15 図 4 は、MAC リストの構成例について説明する図である。

図 5 は、イーサネットフレームのフォーマットを示す図である。

図 6 は、MAC リストに対するクライアント登録処理シーケンスを説明するフロー図である。

図 7 は、MAC リスト登録要求データを説明する図である。

- 20 図 8 は、MAC リストにおけるスロット設定クローズ処理について説明するフロー図である。

図 9 は、データ処理要求に基づく MAC リストへの登録処理を説明するフロー図である。

- 25 図 10 は、UPnP プロトコルに従った処理シーケンスの実行を条件とした MAC リストへの登録処理を説明するフロー図である。

図 11 は、MAC アドレスと他の識別情報の照合処理によるデータ処理実行可否判定を伴うサーバの処理シーケンスを説明するフロー図である。

発明を実施するための最良の形態

以下、図面を参照しながら、本発明の情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラムの詳細について説明する。

5

[システム概要およびMACリスト]

まず、図1を参照して、本発明の適用可能なネットワーク構成例について説明する。図1は、様々なクライアント機器からの処理要求に応じて処理を実行するサーバ101と、サーバ101に対して処理要求を行なうクライアント機器としてのPC121、122、124、PDA、携帯電話等の携帯通信端末123、125がネットワーク100を介して接続された構成、例えばホームネットワーク構成を示している。

サーバ101がクライアントからの要求に応じて実行する処理は、例えばサーバ101の保有するハードディスク等の記憶手段に格納されたコンテンツの提供、あるいはサーバの実行可能なアプリケーションプログラムの実行によるデータ処理サービス等である。なお、図1においては、サーバ101と、その他のクライアント機器としてのPC121、122、124、PDA、携帯電話等の携帯通信端末123、125とを区別して示しているが、クライアントからの要求に対するサービスを提供する機器をサーバとして示しているものであり、いずれのクライアント機器も、自己のデータ処理サービスを他のクライアントに提供する場合には、サーバとしての機能を提供可能となる。従って、図1に示すネットワーク接続されたクライアント機器もサーバとなり得る。

25 ネットワーク100は、有線、無線等いずれかのネットワークであり、各接続機器は、MAC(Media Access Control)アドレスを有している。各ネットワーク接続機器は、宛先MACアドレスおよび送信元MACアドレスをヘッダ情報に持つパケット、例えばイーサネット(登録商標)フレームをネットワーク100を介して送受信する。すなわち、クライアントは、イーサネットフレー

ムのデータ部に処理要求情報を格納したフレームをサーバ101に送信することにより、サーバ101に対するデータ処理要求を実行する。サーバ101は、処理要求フレームの受信に応じて、後述するアクセス権限判定処理を行ない、権限ありの判定を条件としてデータ処理を実行し、必要に応じてデータ処理結果としての結果データをイーサネットフレームのデータ部に格納し、各クライアントに送信する。

ネットワーク接続機器は、例えばユニバーサルプラグアンドプレイ（UPnP：Universal Plug and Play）対応機器によって構成される。従って、ネットワークに対する接続機器の追加、削除が容易な構成である。ネットワークに新たに接続する機器は、

（１）IPアドレス等の自己のデバイスIDを取得するアドレッシング処理。
（２）ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理。

（３）ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理。

上記処理手順を行なうことで、ネットワーク接続された機器を適用したサービスを受領することが可能となる。

図1に示すサーバおよびクライアント機器を構成するPC等の情報処理装置のハードウェア構成例について図2を参照して説明する。

CPU（Central Processing Unit）301は、ROM（Read Only Memory）302、またはHDD304等に記憶されているプログラムに従って、各種の処理を実行し、データ処理手段、あるいは通信制御処理手段として機能する。RAM303には、CPU301が実行するプログラムやデータが適宜記憶される。CPU301、ROM302、およびRAM303、HDD304は、バス305を介して相互に接続されている。

バス 305 には、入出力インタフェース 306 が接続されており、この入出力インタフェース 306 には、例えば、ユーザにより操作されるキーボード、スイッチ、ボテン、あるいはマウス等により構成される入力部 307、ユーザに各種の情報を提示する LCD、CRT、スピーカ等により構成される出力部 308 が接続される。さらに、データ送受信手段として機能する通信部 309、さらに、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどのリムーバブル記録媒体 311 を装着可能で、これらのリムーバブル記録媒体 311 からのデータ読み出しあるいは書き込み処理を実行するドライブ 310 が接続される。

図 2 に示す構成は、図 1 に示すネットワーク接続機器の一例としてのサーバ、パーソナルコンピュータ（PC）の例であるが、ネットワーク接続機器は PC に限らず、図 1 に示すように携帯電話、PDA 等の携帯通信端末、その他の様々な電子機器、情報処理装置によって構成することが可能である。従って、それぞれの機器固有のハードウェア構成を持つことが可能であり、そのハードウェアに従った処理を実行する。

本発明において、アクセス制御を行なうネットワーク接続機器は、アクセス権限を有するネットワーク接続機器の機器リストとしてアクセス権限を有するネットワーク接続機器の MAC アドレスを登録した MAC リストを生成し、格納する。従来においても、MAC リストに基づくアクセス制限構成は存在するが、これは、ユーザが、各ネットワーク接続機器の MAC アドレスを調べ、調べた MAC アドレスを入力してリストを作成する処理を必要としていた。

本発明の構成においては、このようなユーザによる処理を行なうことは必要ではなく、アクセス制御を行なうネットワーク接続機器が、ネットワーク接続機器からのパケット受信に基づいて自動的に MAC リストを作成する。

図3に、アクセス制御を実行するネットワーク接続機器（サーバ）の処理機能を説明するブロック図を示す。サーバは、ネットワークを介したパケットの送受信を実行するパケット送受信部501、パケット送受信部501を介して受信するパケットの解析および、パケット送受信部501を介して送信するパケットを生成するパケット生成、解析部502、クライアントから受信するパケットに基づいてMACリストに対する登録可否を判定する登録可否判定部503、登録可否判定部503の判定に基づいて登録処理を実行する登録処理部504、MACリストを格納した記憶部505、さらに、サーバに対する様々なデータ処理要求パケットに基づいて、データ処理要求クライアントがMACリストに登録されているか否かに基づいてデータ処理の実行可否を判定するデータ処理可否判定部506、データ処理可否判定部におけるデータ処理可の判定を条件として、クライアントの要求するデータ処理を実行するデータ処理部507を有する。

図4に、アクセス制御を実行するネットワーク接続機器（サーバ）に格納されるアクセス制御リストとしてのMACリストの構成例を示す。

MACリストは、サーバ内の記憶部（不揮発性メモリ）に格納される。MACリストは、スロット単位で、各クライアントの登録データを格納する構成を有し、1スロット毎に1つの登録クライアント情報を格納する。

登録情報には、クライアントのMACアドレス、ユーザが任意に設定可能なクライアント名、登録日時が含まれる。さらに、オプションとして、MACアドレスとは異なる識別データ、例えばGUID（Global Unique Identifier）等の固有識別子、あるいは各クライアント機器に設定された鍵データ等を格納してもよい。これらの格納データは、登録処理の際にクライアントから送信されるパケット（イーサネットフレーム）に含まれるデータであり、サーバは、クライアントからの送信パケット（イーサネットフレーム）から登録情報を取得してMACリストに対する登録処理を実行する。

イーサネットフレームの構成を図5に示す。イーサネットフレームは、ヘッダ部、データ部、トレーラ部に区分され、ヘッダ部には、同期信号、パケット開始符号、宛先MACアドレス、送信元MACアドレス、およびパケット長、
5 タイプが含まれる。

データ部には、例えばTCP/IP通信プロトコルに従って生成されたデータが含まれ、例えば送信元、送信先IPアドレスを含むIPパケットが格納される。図4に示すMACリストの登録データ中、MACアドレス情報は、図5
10 に示すイーサネットフレームのヘッダ部に設定される送信元MACアドレスから取得し、その他の情報は、データ部の格納データから取得する。これらの情報を登録処理を実行するサーバ、すなわち、イーサネットフレーム（パケット）を受信したサーバが取得して、パケットから必要情報を読み出して、MACリストに対する登録処理を実行する。

15

図4に示すMACリストは、前述したようにスロット単位で1クライアント情報が格納される。スロット数はユーザが任意に設定可能である。サーバにおいて、クライアント情報を登録する際には、空きスロットがあるか否かを判断し、空きスロットがある場合に限り新規登録が可能となる。図4に示す例では、
20 設定スロット数は、#01～#03の3つであり、スロットNo. #04～は、クローズ状態であるので、最大3つのクライアントを登録可能とした状態を示している。

ユーザは新規のクライアントをネットワークに接続して登録処理を実行する際には、サーバのMACリストに空きスロットを生成する。図4に示す状態は、スロットNo. #01, #02が登録済みスロットであり、スロットNo. #03が空きスロットとして設定され、スロットNo. #03に対して、1つのクライアントのみ新規登録可能な状態である。なお、空きスロットを設定した後、空きスロットは所定時間後に自動的にクローズされる構成としてもよい。

これは、ユーザの予期しない第三者の機器による不正登録の発生を防止するためである。これらの処理については、後述する。

[MACリストに対するクライアント登録処理]

- 5 次に、クライアントのMACリストに対する登録処理手順の基本シーケンスについて、図6の処理フローを用いて説明する。

左側がMACリストに対する登録要求を実行するクライアントの処理を示しており、右側がクライアントからの登録要求を受信しMACリストに対する
10 登録処理を実行するサーバ側の処理を示している。

- クライアントは、ステップS111において、機器の電源をONとする処理、あるいは所定アプリケーション、例えばホームネットワークを利用したサービスの実行アプリケーションを起動する処理のいずれかの処理を実行すると、
15 テップS112において、これらの処理をトリガとして登録処理要求パケットをサーバに対して自動送信する。なお、このパケット送信は、ブロードキャストあるいはマルチキャスト送信として実行される。

- すなわち、クライアントとしての情報処理装置は、制御部、すなわち、図2
20 のハードウェア構成例のCPU301が、記憶部に格納されたプログラムに従って、機器の電源をONとする処理、あるいは所定アプリケーション、例えばホームネットワークを利用したサービスの実行アプリケーションを起動する処理のいずれかの処理を検出し、該検出情報をトリガとして登録処理要求パケット、すなわち、ヘッダにMACアドレスを格納し、サーバの保有するMAC
25 リストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して、サーバに対して自動送信する処理を実行する。

図7に登録要求の際に送信されるメッセージデータのデータ部の主要構成例を示す。「B-POST*HTTP/1.1」は、メッセージの書式がHT

- TPのVer. 1. 1であることを示し、「HOST: 192. 254. 255. 255: 3536」は、ブロードキャスト用のホストのIPアドレスと、ポート番号を示す。「Content-Type: application /...」、「Content-Length: 65」は、コンテンツタイプおよび
5 レンダリングを示し、「Broadcast SNAC」は、ある特定のネットワークアクセスコントロール(SNAC)に従った、ブロードキャスト送信であることを示し、「Method: Register」は、本パケットに従って実行すべき実行メソッドが登録メソッドであることを示している。
- 10 さらに、上記データに加え、図4のMACリストの登録データとして含まれるクライアント名、GUID等のID情報、鍵情報等を含める構成としてもよい。登録処理の際に送信するパケットに格納するデータは、サーバ側のMAC
15 リストに何を登録するかに応じて定義することが可能であり、クライアントは、電源ON時、あるいはホームネットワークを利用したサービスの実行アプリケーションの起動時に、定義情報に従ったデータを格納した登録処理要求パケットを生成し、送信する処理を実行する。

- 図6の処理フローに戻りMACリストに対するクライアント情報登録シーケンスについて説明を続ける。ステップS121において、クライアントから
20 上述したデータを含む登録処理要求パケットを、図3に示すパケット送受信部501を介して受信し、パケット生成、解析部502において、パケット解析を実行し、登録処理要求パケットであることを判別し、登録可否判定部503において登録可否の判定を実行する。

- 25 サーバは、ステップS122において、自己の記憶部505内のMACリストを参照し、受信パケットに含まれる送信元MACアドレスに対応するデータが既に登録済みか否かを判定し、登録済みであれば、処理を終了する。なお、この際、登録済みであることを通知する応答メッセージをクライアント側に送信する処理を実行する構成としてもよい。

ステップ S 1 2 2 において、自己の記憶部 5 0 5 内の MAC リストに、受信
パケットに含まれる送信元 MAC アドレスに対応するデータが登録されてい
ないと判定した場合は、ステップ S 1 2 3 において、MAC リストにデータ登
録可能な空きスロットが存在するか否かを判定する。空きスロットが無い場合
5 は、新規クライアントの登録処理は実行できないので、処理を終了する。なお、
この際、登録不可であることを通知する応答メッセージをクライアント側に送
信する処理を実行する構成としてもよい。

10 ステップ S 1 2 3 において、MAC リストにデータ登録可能な空きスロット
が存在すると判定された場合には、ステップ S 1 2 4 において、図 3 に示す登
録処理部 5 0 4 が、クライアントから受信した登録処理要求パケットのヘダに
含まれる送信元 MAC アドレスおよびデータ部に含まれる登録情報を取得し、
MAC リストの空きスロットに登録する処理を実行する。

15

以上の処理によって、サーバによるクライアントの MAC リストへの登録処
理が終了する。MAC リストに登録されたクライアントは、サーバに対するデ
ータ処理要求を、先に説明したイーサネットフレーム（図 5 参照）等のパケッ
トによりサーバに送信すると、サーバのデータ処理可否判定部 5 0 6（図 3 参
照）ではイーサネットフレームのヘッダ情報から送信元 MAC アドレスを取得
20 し、記憶部 5 0 5 に格納された MAC リストの登録情報との照合を実行し、登
録された MAC アドレスと一致した場合は、データ処理部 5 0 7 において要求
処理を実行、例えばコンテンツの提供等を実行する。

25 クライアントから受信したデータ処理要求フレームのヘッダ情報中の送信
元 MAC アドレスが、記憶部 5 0 5 に格納された MAC リストに登録されてい
ない場合は、不正なクライアントからの処理要求であると判定し、クライアン
トの要求処理は実行しない。

なお、図 6 を参照して説明したMACリストに対するクライアント情報の登録処理は、基本的にスロットに空きスロットがあれば自動登録する処理として説明したが、登録の可否をユーザ自身が判定した後、MACリストに対する登録処理を実行する構成としてもよい。この場合、図 6 の処理ステップのステップS 1 2 3 とステップS 1 2 4 の間で、ユーザによる判定処理ステップを実行することになる。例えば、サーバが受信したパケット情報をディスプレイに表示し、ユーザが表示情報に基づいて、登録可と判定した場合にのみ、入力手段から登録実行コマンドを入力し、ユーザ入力を条件としてMACリストに対する登録を行なう。このような構成によれば、さらにセキュアな登録処理が可能となる。

[空きスロットの自動クローズ処理]

次に、MACリストを格納したサーバにおいて実行されるMACリスト中の空きスロット設定およびスロットのクローズ処理について説明する。前述したように、MACリストはサーバの記憶部にスロット単位で設定され、各スロットに1つのクライアント情報が格納される。

空きスロットの設定、空きスロットのクローズ処理はユーザによる処理によって実行可能である。ただし、空きスロットを設定した後、長時間、空きスロットを放置した場合、上述したユーザ確認を伴わない自動登録処理を実行すると、第三者による不正な登録処理が行われる可能性がある。このような事態を防止するため、設定された空きスロットを予め定められた閾値時間経過後、自動的にクローズする処理を実行する。すなわち、MACリストを保持するサーバの制御部は、MACリストに設定される空きスロット設定からの経過時間を計測し、計測時間が予め設定された閾値時間を経過したことを条件としてクローズ処理を実行する。

空きスロットの設定および自動クローズ処理について、図 8 のフローを参照して説明する。ステップS 2 0 1 において、ユーザによりMACリストに空き

スロットの設定がなされる。通常、ユーザは新たなクライアント機器をネットワークに接続する際、新規接続機器の数に応じて空きスロットを追加設定する。このように必要な数のみのスロットを設定し、不要な空きスロットを設定しないことで、ユーザの管理する機器のみをMACリストに登録することができる。

5

ステップS201の空きスロット設定の後、サーバは、登録処理要求パケットを待機する。これは、図6のフローを参照して説明したクライアントからの登録処理要求パケットであり、例えばクライアントの電源ONまたは、アプリケーション起動に応じて自動送信されるパケットである。

10

サーバは、ステップS201の空きスロットの設定からの経過時間を計測し、ステップS203において予め定めた閾値時間との比較を行なう。ステップS204において、閾値時間内にクライアントからの登録処理要求パケットを受信した場合は、ステップS205において登録処理要求パケットからMACアドレス等の登録情報を取得してMACリストの空きスロットに対する登録処理を実行する。

15

閾値時間内にクライアントからの登録処理要求パケットを受信しなかった場合には、ステップS206に進み、MACリスト中の空きスロットのクローズ処理を実行する。このクローズ処理により、MACリストには空きスロットが存在しなくなり、サーバが第三者からの登録要求を受信した場合においても登録処理を誤って実行することがなくなり、不正なデータ処理要求に応じることが防止される。

20

25 [データ処理要求時の登録処理]

先に図6を参照して説明した新規クライアントのMACリストに対する登録処理は、登録要求を示す登録処理要求パケットをサーバが受信した場合に実行する登録処理であったが、このような明示的な登録要求に応じてMACリストに対する処理を実行するのみならず、通常の前データ処理要求、例えばサーバ

の記憶手段に格納した映像データあるいは音楽データ等のコンテンツ取得要求 packets をクライアントから受信した際に、サーバ側でクライアントの MAC リストに対する自動登録を行なう構成も可能である。

- 5 以下、図 9 のフローを参照して、サーバがクライアントから受信する通常のデータ処理要求に基づいて、データ処理要求クライアントを MAC リストへ登録する処理手順について説明する。

- 10 まず、ステップ S 3 0 1 において、サーバは、クライアントからの登録処理要求 packet またはデータ処理要求 packet を受信すると、ステップ S 3 0 2 において、受信 packet が登録処理要求 packet であるか、データ処理要求 packet であるかを判定する。

- 15 登録処理要求 packet である場合には、ステップ S 3 0 3 において MAC リストの空きスロットの有無を判定し、空きスロットのある場合には受信 packet から登録情報を取得して登録処理を行なう。これは図 6 を参照して説明した処理に相当する。

- 20 一方、ステップ S 3 0 2 の packet 種別判定処理において、データ処理要求 packet であると判定した場合には、ステップ S 3 0 5 において、データ処理要求 packet のヘッダ情報に含まれる送信元 MAC アドレスが記憶部に格納した MAC リストに登録済みか否かを判定する。この処理は、図 3 に示すデータ処理可否判定部 5 0 6 において実行する。

- 25 MAC リストに登録済みであれば、登録されたクライアントからのデータ処理要求であるので、ステップ S 3 0 6 において、要求に従った処理を実行する。データ処理は、図 3 に示すデータ処理部 5 0 7 において実行する。

ステップ S 3 0 5 において、データ処理要求 packet のヘッダ情報に含まれ

る送信元MACアドレスが記憶部に格納したMACリストに登録されていないと判定した場合は、ステップS307において、MACリストの空きスロットの有無を判定し、空きスロットがある場合には、ステップS308において受信パケットから送信元MACアドレス等の登録情報を取得して登録処理を行なう。さらに、登録の後、ステップS306において、クライアントの要求処理を実行して処理を終了する。

このように、クライアントから受信する通常のデータ処理要求に応じてサーバ側で未登録のクライアントを登録する処理を実行する構成によれば、特別な登録処理要求パケットの送受信処理を必要とすることなくMACリストへのクライアント登録が可能となる。

なお、図9を参照して説明したMACリストに対するクライアント情報の登録処理は、基本的にスロットに空きスロットがあれば自動登録する処理として説明したが、この処理においても先に説明した図6の登録処理要求パケットに対する処理と同様、登録の可否をユーザ自身が判定した後、MACリストに対する登録処理を実行する構成としてもよい。この場合、図9の処理ステップのステップS307とステップS308の間にユーザによる判定処理ステップを実行することになる。例えば、サーバが受信したパケット情報をディスプレイに表示し、ユーザが表示情報に基づいて、登録可と判定した場合にのみ、入力手段から登録実行コマンドを入力し、ユーザ入力を条件としてMACリストに対する登録を行なう。このような構成によれば、さらにセキュアな登録処理が可能となる。

25 [UPnPプロトコルに対応するパケットに対する登録処理]

上述したクライアントからの登録処理要求パケットまたはデータ処理要求パケットに基づくサーバにおけるMACリストへの登録処理を実行する場合には、クライアントからの登録処理要求パケットまたはデータ処理要求パケットが、ある特定のネットワークアクセスコントロール(SNAC)に従ったパ

ケットであることを、サーバにおいて認識することが必要となる。従って、このような特定のネットワークアクセスコントロール(SNAC)に従ったパケットを送信できない機器については、上述した受信パケットに基づくMACリストに対する登録処理ができないことになる。

5

前述したように、ホームネットワーク等においては、簡易な機器のネットワーク接続を可能としたユニバーサルプラグアンドプレイ(UPnP:Universal Plug and Play)対応機器が接続されることが多く、UPnP対応機器は、様々なメーカーにおいて製造されており、既に多くの機器が実在する。

10

そこで、特定のネットワークアクセスコントロール(SNAC)に従ったパケットを送信できないUPnP対応機器についてもMACリストへの自動登録を可能とする構成例について、以下説明する。

15

本実施例は、サーバが、クライアントから受信するパケットに基づいて実行する処理を解析し、UPnPプロトコルに従ったシーケンスが的確に実行されているか否かを判定する。UPnPプロトコルに従ったシーケンスが的確に実行されているとの判定を条件として、そのUPnP対応機器をMACリストへ登録する処理を実行する。なお、この判定条件として、UPnP AVプロトコルに従ったシーケンスが的確に実行されているかを採用してもよい。この場合、UPnPプロトコルは搭載する可能性はあるが、UPnP AVプロトコルを搭載しないであろう照明器具からの登録を排除することができる。

20

25

図10に本実施例に従ったサーバの処理シーケンスを説明するフローチャートを示す。サーバは、ステップS401においてクライアントから処理要求パケットを受信し、ステップS402において、UPnPプロトコルに従った処理シーケンスが的確に実行されているか否かを判定する。

前述したように、UPnPプロトコルに従った処理シーケンスは、基本的に

下記ステップから構成される。

(1) IPアドレス等の自己のデバイスIDを取得するアドレッシング処理ステップ。

5 (2) ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理ステップ。

(3) ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理ステップ。

10 サーバは、上述の処理ステップが的確に実行されていれば、正当なUPnP対応のクライアント機器であると判断し、MACリストへの登録可能機器であると判定する。上記(1)～(3)の処理が実行されない場合には、登録不可と判定(S402:No)し、処理を終了する。

15 上述の処理ステップが的確に実行されており、正当なUPnP対応のクライアント機器であると判定した場合は、ステップS403において、データ処理要求パケットのヘッダ情報に含まれる送信元MACアドレスが記憶部に格納したMACリストに登録済みか否かを判定する。この処理は、図3に示すデータ処理可否判定部506において実行する。

20

MACリストに登録済みであれば、登録されたクライアントからのデータ処理要求であるので、ステップS406において、要求に従った処理を実行する。データ処理は、図3に示すデータ処理部507において実行する。

25 ステップS403において、データ処理要求パケットのヘッダ情報に含まれる送信元MACアドレスが記憶部に格納したMACリストに登録されていないと判定した場合は、ステップS404において、MACリストの空きスロットの有無を判定し、空きスロットがある場合には、ステップS405において受信パケットから登録情報を取得して登録処理を行なう。さらに、登録の後、

ステップS 4 0 6において、クライアントの要求処理を実行して処理を終了する。

このように、本実施例に従えば、クライアントが、特定のネットワークアクセスコントロール（SNAC）に従ったパケットを送信できない機器であっても、ユニバーサルプラグアンドプレイ（UPnP：Universal Plug and Play）対応機器であり、UPnPプロトコルに従ったシーケンスを確実に実行している場合には、MACリストへの自動登録が可能となり、ユーザの負担を発生させることのないMACリスト生成が可能となる。

なお、サーバにおけるUPnPプロトコルに従った処理シーケンスが的確に実行されているか否かの判定レベルとしては様々な設定が可能である。例えば、コンテンツを提供するサービスを実行するサーバにおいては、UPnPプロトコルに従ったコンテンツリスト要求処理、いわゆるコンテンツディレクトリサービス（CDS）要求処理まで実行されたことを条件としてMACリストへの登録条件として設定する。

すなわち、コンテンツを提供するサービスを実行するサーバにおいては、UPnPプロトコルに従った処理シーケンス中、コンテンツリスト要求処理、いわゆるコンテンツディレクトリサービス（CDS）要求処理が実行された場合に、サーバの保持するMACリストへの登録対象クライアントであると判定して登録処理を実行し、コンテンツディレクトリサービス（CDS）要求処理が実行されない場合には、サーバの保持するMACリストへの登録対象クライアントではないと判定して登録処理を実行しない。

このように、サーバの提供するサービスに対応するUPnPプロトコルシーケンスの実行がなされたことを条件としてMACリストへの登録を実行することにより、リスト登録の不要なクライアント機器をMACリストに登録してしまうといった無駄な登録処理を防止することができる。

[識別子 (ID)、鍵情報に基づく認証]

先に図 4 を参照して説明したように、MAC リストのクライアント登録情報には、MAC アドレス、クライアント名、登録日時の他にオプションとしてグローバルユニークな識別子としての GUID や、機器に対して設定された固有の鍵情報データを格納することが可能である。

このような MAC アドレス以外の識別情報は、よりセキュアな管理を実現するために適用される。MAC アドレスは通常 48 ビットデータであり、このデータは、一般ユーザも機器を調べることにより取得可能な情報であって基本的に秘密とされているわけではない。従って、不正を実行しようとするれば、正当なクライアント機器になりすまし、正当な機器の MAC アドレスを、他の不正な機器の MAC アドレスとして適用して不正機器を MAC リストに登録してしまう事態も発生しないとは言えない。

比較的データ量の少ない 48 ビット MAC アドレスのみをクライアント確認の条件データとして適用するのではなく、さらにデータ量の多い識別データあるいは漏洩の可能性の少ないデータ等をクライアント確認のために適用することにより、高いレベルでのセキュリティ管理が実現される。

登録要求を行なうクライアントは、登録処理要求パケット、またはデータ処理要求パケットのデータ部にグローバルユニークな識別子としての GUID (例えば 128 ビット以上のデータ) や、機器に対して設定された固有の鍵情報データを格納し、サーバに送信する。サーバは、MAC アドレス、クライアント名、登録日時の他に、データ部に格納された GUID や、機器に対して設定された固有の鍵情報データを取り出して MAC リストの登録情報として設定する。

登録後のクライアントからのデータ処理要求において、クライアントは登録

されているGUID、鍵情報等の識別データをパケットに格納したデータ処理要求パケットを生成してサーバに送信する。サーバは、データ処理要求パケットに含まれるMACアドレスと、GUID、鍵情報等の識別データを取得して、MACリストに登録された各データと一致するか否かを判定し、一致した場合にのみサービスを提供する。

図11を参照して、MACアドレス以外の識別情報の照合を条件としてサービス提供を実行する場合のサーバにおける処理シーケンスについて説明する。

10 ステップS501において、クライアントからのデータ処理要求パケットを受信すると、ステップS502において、パケットのヘッダ部に設定された送信元MACアドレスと、データ部に格納されたGUID鍵情報等の識別情報を取得する。ステップS503において、パケットのヘッダ部に設定された送信元MACアドレスと、MACリストに登録された登録情報との照合を実行し、
15 一致しない場合は、未登録クライアントからの処理要求であると判定し、要求処理を実行しないで終了する。

MACアドレスの照合に成功し、一致する登録情報があった場合は、ステップS504において、パケットのデータ部に格納された識別情報と、MACリスト中の照合MACアドレスの格納された同一スロット中の識別情報との照
20 合処理を実行する。

識別情報が一致しない場合は、不正クライアントからの処理要求であると判定し、要求処理を実行しないで終了する。識別情報が一致した場合は、ステップS505においてクライアントの要求処理を実行する。
25

上述した処理によれば、データ処理要求を受信したサーバが、MACアドレスのみならず、データ量の多い識別データあるいは漏洩の可能性の少ないデータ等を用いてクライアント確認を実行することが可能となり、高いレベルでの

セキュリティ管理が実現される。

5 なお、上述の実施の形態では、MACアドレスをクライアント識別情報として説明したが、クライアント識別情報としてCPUのID、デバイスのシリアルナンバーまたはニックネーム、その他のデバイスを識別可能な情報を用いることもできる。

10 以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

15 なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

20

25 例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory) に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical) ディスク, DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュー

タにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体に
5 インストールすることができる。

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数
10 の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

産業上の利用可能性

15 以上、説明したように、本発明によれば、ネットワークに接続されたクライアント機器の電源をONとする処理、あるいは所定アプリケーション、例えばホームネットワークを利用したサービスの実行アプリケーションを起動する処理のいずれかの処理をトリガとして、MACリスト登録処理要求パケットを自動送信し、サーバ側で、MACリストの空きスロットの状況に応じて、受信
20 パケットからMACアドレス等の情報を取得して登録する処理を実行する構成としたので、ユーザの負担を発生させることなくアクセス制御リストとしてのMACリストが容易に、かつ効率的に生成可能となる。

また、本発明の構成によれば、サーバにMACリストの空きスロットを設定
25 した後、閾値時間内にクライアントからの登録処理要求パケットを受信しなかった場合には、MACリスト中の空きスロットのクローズ処理を実行する構成としたので、MACリストの空きスロットを放置することがなくなり、サーバが第三者からの登録要求を受信した場合においても登録処理を誤って実行することがなくなり、不正なデータ処理要求に応じることが防止される。

さらに、本発明の構成によれば、クライアントから受信する通常のリクエスト処理要求に応じてサーバ側で未登録のクライアントを登録する処理を実行する構成としたので、登録処理要求パケットを適用することなくMACリストへのクライアント登録が可能となる。

さらに、本発明の構成によれば、クライアントが、特定のネットワークアクセスコントロール(SNAC)に従ったパケットを送信できない機器であっても、ユニバーサルプラグアンドプレイ(UPnP: Universal Plug and Play)対応機器であり、UPnPプロトコルに従ったシーケンスを確実に実行している場合には、MACリストへの自動登録が可能となり、ユーザの負担を発生させることのないMACリスト生成が可能となる。

さらに、本発明の構成によれば、MACリストの登録情報としてグローバルユニークな識別子としてのGUIDや、機器に対して設定された固有の鍵情報データを格納し、データ処理要求を受信したサーバが、MACアドレスのみならず、GUIDや鍵情報等の識別データを用いてクライアント確認を実行することが可能となり、高いレベルでのセキュリティ管理が実現される。

請求の範囲

1. アクセス制御リストの生成処理を実行する情報処理装置であり、
 - 5 アクセス要求機器としてのクライアントからのパケットを受信する受信部と、
1 1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストを格納した記憶部と、
10 前記受信部における受信パケットに基づくクライアント登録処理に際して、前記MACリストの空きスロットの有無を確認し、空きスロットがある場合にのみ登録可能とする判定を行なう登録可否判定部と、
15 前記登録可否判定部における登録可能の判定に基づいて、前記受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する登録処理部と、
20 を有することを特徴とする情報処理装置。
2. 前記登録処理部は、
前記クライアントからの受信パケットのヘッダ部に含まれる送信元MACアドレスを取得し、前記MACリストに対する登録情報として適用する処理を
20 実行する構成であることを特徴とする請求項1に記載の情報処理装置。
3. 前記情報処理装置は、さらに、
クライアントからの受信パケットが登録処理要求パケットであるかデータ
処理要求であるかを判別するパケット解析部を有し、
25 前記登録可否判定部は、クライアントからの受信パケットが登録処理要求パケットである場合に、前記MACリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、
前記登録処理部は、前記登録可否判定部における登録可能の判定に基づく登録処理を実行する構成であることを特徴とする請求項1に記載の情報処理装

置。

4. 前記情報処理装置において、

前記登録可否判定部は、クライアントからの受信パケットがデータ処理要求
5 パケットである場合に、前記MACリストの空きスロット有無検出処理に基づ
く登録可否判定処理を実行し、

前記登録処理部は、前記登録可否判定部における登録可能の判定に基づいて、
受信したデータ処理要求パケットからクライアントMACアドレスを含むデ
ータを取得し、前記MACリストに対する登録処理を実行する構成であること
10 を特徴とする請求項1に記載の情報処理装置。

5. 前記情報処理装置は、さらに、

前記MACリストの空きスロットの設定処理からの経過時間が予め定めら
れた閾値時間を経過したことを条件として、空きスロットのクローズ処理を実
15 行する制御部を有することを特徴とする請求項1に記載の情報処理装置。

6. 前記登録可否判定部は、

クライアントからのデータ処理要求シーケンスが、UPnPプロトコルに従
ったシーケンスを確実に実行しているか否かを判定する処理を実行する構成
20 を有し、

前記登録処理部は、

クライアントからのデータ処理要求シーケンスが、UPnPプロトコルに従
ったシーケンスを確実に実行しているとの判定に基づいて、クライアントから
の受信パケットからクライアントMACアドレスを含むデータを取得し、前記
25 MACリストに対する登録処理を実行する構成であることを特徴とする請求
項1に記載の情報処理装置。

7. 前記登録可否判定部は、

クライアントからのデータ処理要求において、UPnPプロトコルに従った

シーケンス中のコンテンツディレクトリサービス（CDS）要求処理が実行されたか否かを判定し、

前記登録処理部は、

前記コンテンツディレクトリサービス（CDS）要求処理が実行されたとの

- 5 判定に基づいて、クライアントからの受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

8. 前記登録処理部は、

- 10 クライアントからの受信パケットに格納されたMACアドレスおよびMACアドレスと異なる識別情報を取得し、前記MACリストに対する登録処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

- 15 9. 前記MACアドレスと異なる識別情報は、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別情報であることを特徴とする請求項8に記載の情報処理装置。

10. ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置であり、

- 20 自己のMACアドレスをヘッダ情報中に格納し、前記サーバの保有するMACリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行する制御部を有することを特徴とする情報処理装置。

- 25 11. 前記制御部は、

前記アクセス制御リスト登録処理要求パケットの生成処理において、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別情報を格納したパケット生成処理を実行する構成であることを特徴とする請求項10に記載の情報処理装置。

1 2. 前記制御部は、

前記アクセス制御リスト登録処理要求パケットをブロードキャスト送信またはマルチキャスト送信として実行する構成であることを特徴とする請求項

5 1 0 に記載の情報処理装置。

1 3. アクセス要求を受信するサーバと、アクセス要求を実行するクライアントからなるサーバクライアントシステムにおいて、

前記クライアントは、

10 自己のMACアドレスをヘッダ情報中に格納したアクセス制御リスト登録処理要求パケットを、情報処理装置の電源オン処理、または特定アプリケーション起動処理を条件として生成し、送信処理を実行する構成を有し、

前記サーバは、

15 前記クライアントからのアクセス制御リスト登録処理要求パケットを受信し、1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストの空きスロットの有無を確認し、空きスロットがある場合にのみ、前記パケットに基づくクライアント情報の、前記MACリストに対する登録処理を実行する構成を有する、

ことを特徴とするサーバクライアントシステム。

20

1 4. 前記サーバは、

前記クライアントからの受信パケットのヘッダ部に含まれる送信元MACアドレスを取得し、前記MACリストに対する登録情報として適用する処理を実行する構成であることを特徴とする請求項1 3に記載のサーバクライアント

25 トシステム。

1 5. アクセス制御リストの生成処理を実行する情報処理方法であり、

アクセス要求機器としてのクライアントからのパケットを受信する受信ステップと、

1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストの空きスロットの有無を判定する登録可否判定ステップと、

- 前記登録可否判定ステップにおける空きスロット有りの判定に基づいて、前記受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する登録処理ステップと、
- 5 有することを特徴とする情報処理方法。

16. 前記登録処理ステップは、

- 10 前記クライアントからの受信パケットのヘッダ部に含まれる送信元MACアドレスを取得し、前記MACリストに対する登録情報として適用する処理を実行することを特徴とする請求項15に記載の情報処理方法。

17. 前記情報処理方法は、さらに、

- 15 クライアントからの受信パケットが登録処理要求パケットであるかデータ処理要求であるかを判別するパケット解析ステップを有し、

前記登録可否判定ステップは、前記パケット解析ステップにおける解析結果がクライアントからの受信パケットが登録処理要求パケットであると判定された場合に、前記MACリストの空きスロット有無検出処理に基づく登録可否

- 20 判定処理を実行することを特徴とする請求項15に記載の情報処理方法。

18. 前記情報処理方法において、

前記登録可否判定ステップは、

- 25 クライアントからの受信パケットがデータ処理要求パケットである場合においても、前記MACリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、

前記登録処理部ステップは、

前記登録可否判定部における登録可能の判定に基づいて、受信したデータ処理要求パケットからクライアントMACアドレスを含むデータを取得し、前記

MACリストに対する登録処理を実行することを特徴とする請求項15に記載の情報処理方法。

19. 前記情報処理方法は、さらに、

- 5 前記MACリストの空きスロットの設定処理からの経過時間が予め定められた閾値時間を経過したことを条件として、空きスロットのクローズ処理を実行する制御ステップを有することを特徴とする請求項15に記載の情報処理方法。

- 10 20. 前記登録可否判定ステップは、

クライアントからのデータ処理要求シーケンスが、UPnPプロトコルに従ったシーケンスを確実に実行しているか否かを判定する処理を実行するステップを含み、

前記登録処理ステップは、

- 15 クライアントからのデータ処理要求シーケンスが、UPnPプロトコルに従ったシーケンスを確実に実行しているとの判定に基づいて、クライアントからの受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行することを特徴とする請求項15に記載の情報処理方法。

20

21. 前記登録可否判定ステップは、

クライアントからのデータ処理要求において、UPnPプロトコルに従ったシーケンス中のコンテンツディレクトリサービス(CDS)要求処理が実行されたか否かを判定するステップを含み、

- 25 前記登録処理ステップは、

前記コンテンツディレクトリサービス(CDS)要求処理が実行されたとの判定に基づいて、クライアントからの受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行することを特徴とする請求項15に記載の情報処理方法。

22. 前記登録処理ステップは、

クライアントからの受信パケットに格納されたMACアドレスおよびMACアドレスと異なる識別情報を取得し、前記MACリストに対する登録処理を
5 実行することを特徴とする請求項15に記載の情報処理方法。

23. 前記MACアドレスと異なる識別情報は、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別情報であることを特徴とする請求項22に記載の情報処理方法。

10

24. ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置における情報処理方法であり、

情報処理装置の電源オン処理、または特定アプリケーション起動処理をトリガ情報として検出するトリガ検出ステップと、

15 前記トリガ情報の検出を条件として、自己のMACアドレスをヘッダ情報中に格納し、前記サーバの保有するMACリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行するパケット生成送信処理ステップと、

を有することを特徴とする情報処理方法。

20

25. 前記パケット生成送信処理ステップは、

前記アクセス制御リスト登録処理要求パケットの生成処理において、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別情報を格納したパケット生成処理を実行することを特徴とする請求項
25 24に記載の情報処理方法。

26. 前記パケット生成送信処理ステップは、

前記アクセス制御リスト登録処理要求パケットをブロードキャスト送信またはマルチキャスト送信として実行することを特徴とする請求項24に記載

の情報処理方法。

27. アクセス制御リストの生成処理を実行するコンピュータプログラムであり、

- 5 アクセス要求機器としてのクライアントからのパケットを受信する受信ステップと、

1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストの空きスロットの有無を判定する登録可否判定ステップと、

- 10 前記登録可否判定ステップにおける空きスロット有りの判定に基づいて、前記受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する登録処理ステップと、
を有することを特徴とするコンピュータ・プログラム。

- 15 28. ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置における情報処理方法を実行するコンピュータプログラムであり、

情報処理装置の電源オン処理、または特定アプリケーション起動処理をトリガ情報として検出するトリガ検出ステップと、

- 20 前記トリガ情報の検出を条件として、自己のMACアドレスをヘッダ情報中に格納し、前記サーバの保有するMACリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行するパケット生成送信処理ステップと、
を有することを特徴とするコンピュータ・プログラム。

補正書の請求の範囲

[2004年3月22日(22.03.2004)国際事務局受理 : 出願当初の
請求の範囲1、10、13、15、24、27及び28は補正された;
他の請求の範囲は変更なし。(9頁)]

1. (変更あり)

複数の機器が接続されたネットワークに接続し、アクセス制御リストの生成

5 処理を実行する情報処理装置であり、

アクセス要求機器としてのクライアントからのパケットを前記ネットワークを介して受信する受信部と、

1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストを格納した記憶部と、

10 前記受信部における受信パケットに基づくクライアント登録処理に際して、前記MACリストの空きスロットの有無を確認し、空きスロットがある場合にのみ登録可能とする判定を行なう登録可否判定部と、

前記登録可否判定部における登録可能の判定に基づいて、前記受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに

15 対する登録処理を実行する登録処理部と、

を有することを特徴とする情報処理装置。

2. (変更なし)

前記登録処理部は、

20 前記クライアントからの受信パケットのヘッダ部に含まれる送信元MACアドレスを取得し、前記MACリストに対する登録情報として適用する処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

3. (変更なし)

25 前記情報処理装置は、さらに、

クライアントからの受信パケットが登録処理要求パケットであるかデータ処理要求であるかを判別するパケット解析部を有し、

前記登録可否判定部は、クライアントからの受信パケットが登録処理要求パケットである場合に、前記MACリストの空きスロット有無検出処理に基づく

登録可否判定処理を実行し、

前記登録処理部は、前記登録可否判定部における登録可能の判定に基づく登録処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

5

4. (変更なし)

前記情報処理装置において、

前記登録可否判定部は、クライアントからの受信パケットがデータ処理要求パケットである場合に、前記MACリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、

10

前記登録処理部は、前記登録可否判定部における登録可能の判定に基づいて、受信したデータ処理要求パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

15

5. (変更なし)

前記情報処理装置は、さらに、

前記MACリストの空きスロットの設定処理からの経過時間が予め定められた閾値時間を経過したことを条件として、空きスロットのクローズ処理を実行する制御部を有することを特徴とする請求項1に記載の情報処理装置。

20

6. (変更なし)

前記登録可否判定部は、

クライアントからのデータ処理要求シーケンスが、UPnPプロトコルに従ったシーケンスを確実に実行しているか否かを判定する処理を実行する構成を有し、

25

前記登録処理部は、

クライアントからのデータ処理要求シーケンスが、UPnPプロトコルに従ったシーケンスを確実に実行しているとの判定に基づいて、クライアントから

の受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

5 7. (変更なし)

前記登録可否判定部は、

クライアントからのデータ処理要求において、UPnPプロトコルに従ったシーケンス中のコンテンツディレクトリサービス(CDS)要求処理が実行されたか否かを判定し、

10 前記登録処理部は、

前記コンテンツディレクトリサービス(CDS)要求処理が実行されたとの判定に基づいて、クライアントからの受信パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

15

8. (変更なし)

前記登録処理部は、

クライアントからの受信パケットに格納されたMACアドレスおよびMACアドレスと異なる識別情報を取得し、前記MACリストに対する登録処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

20

9. (変更なし)

前記MACアドレスと異なる識別情報は、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別情報であることを特徴とする請求項8に記載の情報処理装置。

25

10. (変更あり)

ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置であり、

前記ネットワークにおける通信処理が起動されたことを検出する処理起動検出部と、前記処理起動検出部により検出された検出情報をトリガとして、自己のMACアドレスをヘッダ情報中に格納し、前記サーバの保有するMACリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求5 パケットを生成して送信する処理を実行する制御部を有することを特徴とする情報処理装置。

1 1. (変更なし)

前記制御部は、

10 前記アクセス制御リスト登録処理要求パケットの生成処理において、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別情報を格納したパケット生成処理を実行する構成であることを特徴とする請求項10に記載の情報処理装置。

15 1 2. (変更なし)

前記制御部は、

前記アクセス制御リスト登録処理要求パケットをブロードキャスト送信またはマルチキャスト送信として実行する構成であることを特徴とする請求項10に記載の情報処理装置。

20

1 3. (変更あり)

複数の機器が接続されたネットワークに接続しアクセス要求を受信するサーバと、アクセス要求を実行するクライアントからなるサーバクライアントシステムにおいて、

25 前記クライアントは、電源オン処理、または特定アプリケーション起動に基づいて前記ネットワークにおける通信処理が起動されたことを検出し、該検出情報をトリガとして、自己のMACアドレスをヘッダ情報中に格納したアクセス制御リスト登録処理要求パケットを生成して送信する構成を有し、

前記サーバは、前記ネットワークを介して前記クライアントからのアクセス

制御リスト登録処理要求パケットを受信し、1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストの空きスロットの有無を確認し、空きスロットがある場合にのみ、前記パケットに基づくクライアント情報の、前記MACリストに対する登録処理を実行する

5 構成を有する、

ことを特徴とするサーバクライアントシステム。

14. (変更なし)

前記サーバは、

10 前記クライアントからの受信パケットのヘッダ部に含まれる送信元MACアドレスを取得し、前記MACリストに対する登録情報として適用する処理を実行する構成であることを特徴とする請求項13に記載のサーバクライアントシステム。

15 15. (変更あり)

アクセス制御リストの生成処理を実行する情報処理方法であり、

複数の機器が接続されたネットワークに接続し、アクセス要求機器としてのクライアントからのパケットを前記ネットワークを介して受信する受信ステップと、

20 1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストの空きスロットの有無を判定する登録可否判定ステップと、

前記登録可否判定ステップにおける空きスロット有りの判定に基づいて、前記受信パケットからクライアントMACアドレスを含むデータを取得し、前記

25 MACリストに対する登録処理を実行する登録処理ステップと、

を有することを特徴とする情報処理方法。

16. (変更なし)

前記登録処理ステップは、

前記クライアントからの受信パケットのヘッダ部に含まれる送信元MACアドレスを取得し、前記MACリストに対する登録情報として適用する処理を実行することを特徴とする請求項15に記載の情報処理方法。

5 17. (変更なし)

前記情報処理方法は、さらに、

クライアントからの受信パケットが登録処理要求パケットであるかデータ処理要求であるかを判別するパケット解析ステップを有し、

10 前記登録可否判定ステップは、前記パケット解析ステップにおける解析結果がクライアントからの受信パケットが登録処理要求パケットであると判定された場合に、前記MACリストの空きスロット有無検出処理に基づく登録可否判定処理を実行することを特徴とする請求項15に記載の情報処理方法。

18. (変更なし)

15 前記情報処理方法において、

前記登録可否判定ステップは、

クライアントからの受信パケットがデータ処理要求パケットである場合においても、前記MACリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、

20 前記登録処理部ステップは、

前記登録可否判定部における登録可能の判定に基づいて、受信したデータ処理要求パケットからクライアントMACアドレスを含むデータを取得し、前記MACリストに対する登録処理を実行することを特徴とする請求項15に記載の情報処理方法。

25

19. (変更なし)

前記情報処理方法は、さらに、

前記MACリストの空きスロットの設定処理からの経過時間が予め定められた閾値時間を経過したことを条件として、空きスロットのクローズ処理を実

行する制御ステップを有することを特徴とする請求項 15 に記載の情報処理方法。

20. (変更なし)

5 前記登録可否判定ステップは、

クライアントからのデータ処理要求シーケンスが、UPnP プロトコルに従ったシーケンスを確実に実行しているか否かを判定する処理を実行するステップを含み、

前記登録処理ステップは、

10 クライアントからのデータ処理要求シーケンスが、UPnP プロトコルに従ったシーケンスを確実に実行しているとの判定に基づいて、クライアントからの受信パケットからクライアント MAC アドレスを含むデータを取得し、前記 MAC リストに対する登録処理を実行することを特徴とする請求項 15 に記載の情報処理方法。

15

21. (変更なし)

前記登録可否判定ステップは、

クライアントからのデータ処理要求において、UPnP プロトコルに従ったシーケンス中のコンテンツディレクトリサービス (CDS) 要求処理が実行されたか否かを判定するステップを含み、

20

前記登録処理ステップは、

前記コンテンツディレクトリサービス (CDS) 要求処理が実行されたとの判定に基づいて、クライアントからの受信パケットからクライアント MAC アドレスを含むデータを取得し、前記 MAC リストに対する登録処理を実行することを特徴とする請求項 15 に記載の情報処理方法。

25

22. (変更なし)

前記登録処理ステップは、

クライアントからの受信パケットに格納された MAC アドレスおよび MA

Cアドレスと異なる識別情報を取得し、前記MACリストに対する登録処理を実行することを特徴とする請求項15に記載の情報処理方法。

23. (変更なし)

- 5 前記MACアドレスと異なる識別情報は、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる識別情報であることを特徴とする請求項22に記載の情報処理方法。

24. (変更あり)

- 10 ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置における情報処理方法であり、

情報処理装置の電源オン処理、または特定アプリケーション起動に基づいて前記ネットワークにおける通信処理が起動されたことを検出するトリガ検出ステップと、

- 15 前記トリガ情報の検出を条件として、自己のMACアドレスをヘッダ情報中に格納し、前記サーバの保有するMACリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行するパケット生成送信処理ステップと、

を有することを特徴とする情報処理方法。

20

25. (変更なし)

前記パケット生成送信処理ステップは、

前記アクセス制御リスト登録処理要求パケットの生成処理において、グローバルユニークなID情報、またはクライアント機器に設定された鍵情報からなる

- 25 識別情報を格納したパケット生成処理を実行することを特徴とする請求項24に記載の情報処理方法。

26. (変更なし)

前記パケット生成送信処理ステップは、

前記アクセス制御リスト登録処理要求パケットをブロードキャスト送信またはマルチキャスト送信として実行することを特徴とする請求項 24 に記載の情報処理方法。

5 27. (変更あり)

アクセス制御リストの生成処理を実行するコンピュータ・プログラムであり、複数の機器が接続されたネットワークに接続し、アクセス要求機器としてのクライアントからのパケットを前記ネットワークを介して受信する受信ステップと、

- 10 1つのクライアントのMACアドレスを含む情報を1つのスロットの登録データとして設定したMACリストの空きスロットの有無を判定する登録可否判定ステップと、

前記登録可否判定ステップにおける空きスロット有りの判定に基づいて、前記受信パケットからクライアントMACアドレスを含むデータを取得し、前記

- 15 MACリストに対する登録処理を実行する登録処理ステップと、
 を有することを特徴とするコンピュータ・プログラム。

 28. (変更あり)

- 20 ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置における情報処理方法を実行するコンピュータ・プログラムであり、

情報処理装置の電源オン処理、または特定アプリケーション起動に基づいて前記ネットワークにおける通信処理が起動されたことを検出するトリガ検出ステップと、

- 25 前記トリガ情報の検出を条件として、自己のMACアドレスをヘッダ情報中に格納し、前記サーバの保有するMACリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行するパケット生成送信処理ステップと、

 を有することを特徴とするコンピュータ・プログラム。

条約19条(1)に基づく説明書

(1) 請求の範囲第1項、第15項、第27項の補正について、

上記補正は、「アクセス制御リストとしてのMACリストの生成処理を実行する情報処理装置が、複数の機器が接続されたネットワークに接続し、アクセス要求機器としてのクライアントからのパケットを前記ネットワークを介して受信して、受信パケットに基づいてMACリストへの登録処理を実行する構成であること」を明確にした補正である。

本補正は、明細書第15頁25-29行他の記載に基づくものである。

国際調査報告に示された特開2002-159053号公報には基地局および端末におけるユーザ操作によるMACアドレス等の情報登録処理構成が開示され、特開平9-233111号公報には通信処理装置の周辺制御部に回線制御部のMACアドレステーブルを設けて管理し、回線制御部交換時のMACアドレスの復元を可能とした構成を開示している。本発明は、サーバがネットワークを介して接続されているクライアントからのパケット受信に基づいてMACアドレスを自動登録可能としたものであり、ユーザ操作を不要としてMACリストの自動更新が可能となる点で各従来技術とは異なる。

(2) 請求の範囲第10項、第24項、第28項の補正について、

上記補正は、「サーバに対するアクセス要求を実行するクライアントとしての情報処理装置が、ネットワークにおける通信処理が起動されたことを検出し、検出情報をトリガとしてMACアドレスを格納した登録要求パケットを生成、送信する構成」であることを明確にした補正である。

本補正は、明細書第20頁19-26行他の記載に基づくものである。

(3) 請求の範囲第13項の補正について、

請求の範囲第13項の補正は、上記(1)、(2)の両補正を含む補正を行なったものである。

以上

1/11

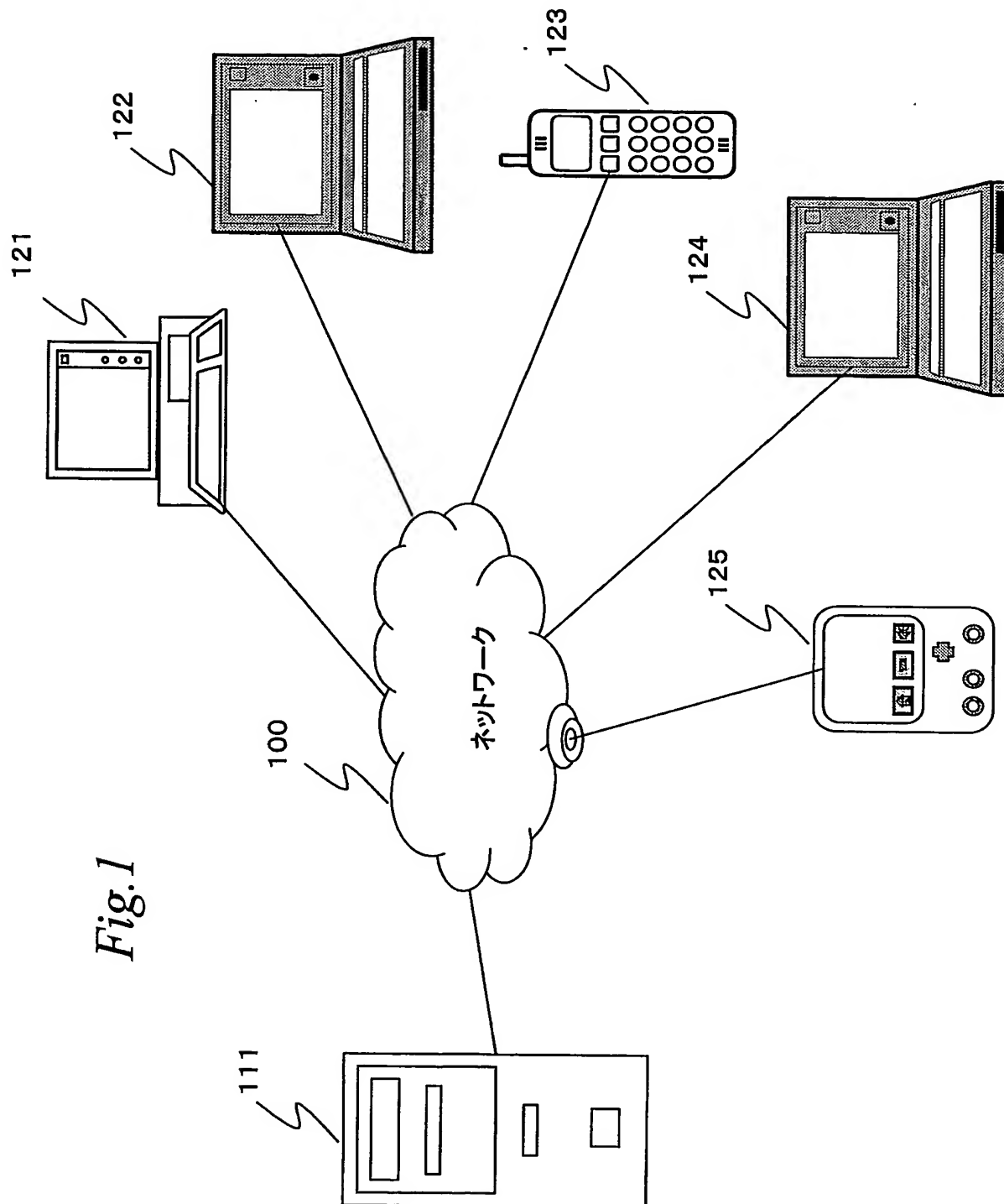


Fig. 1

2/11

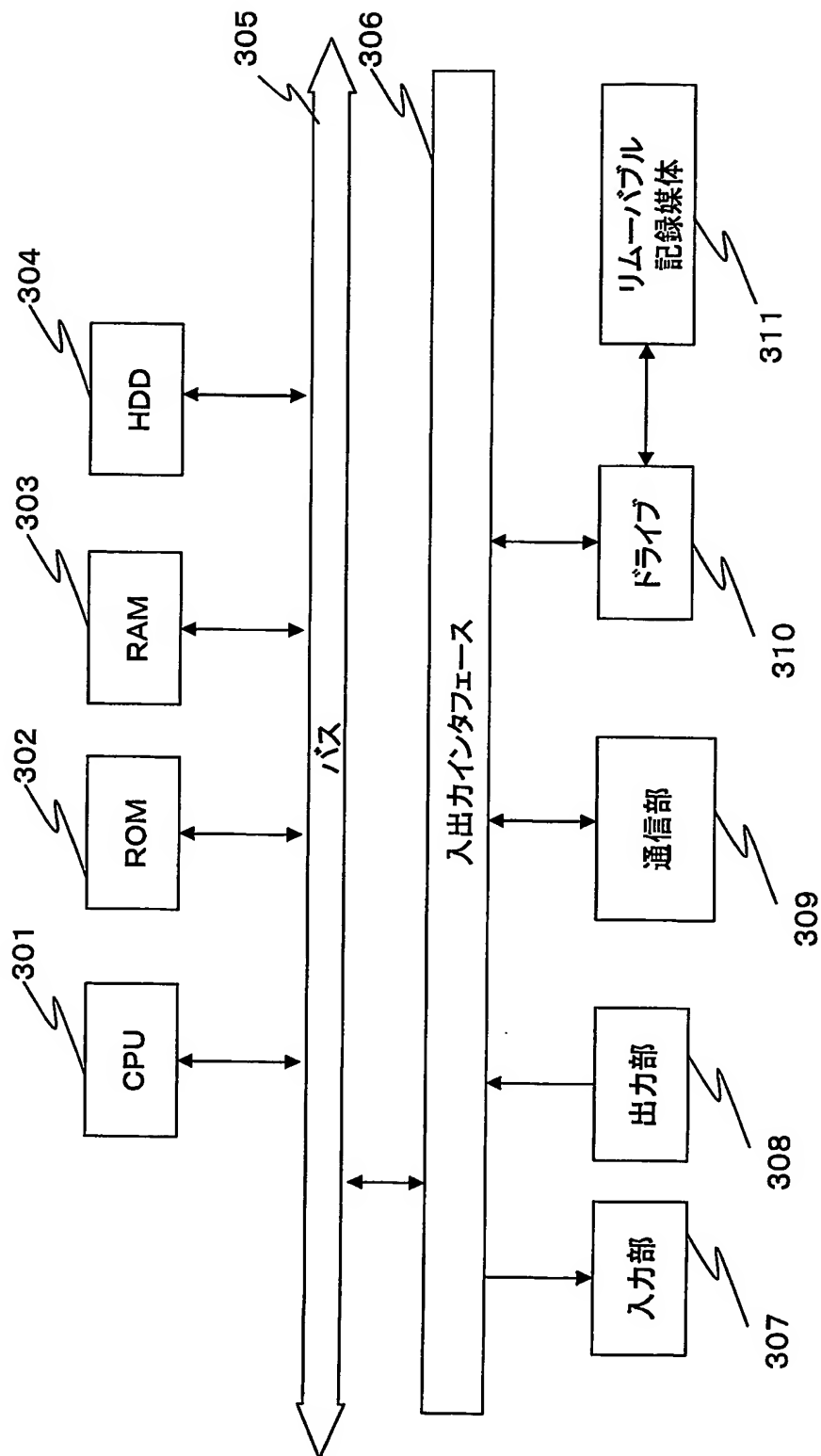


Fig.2

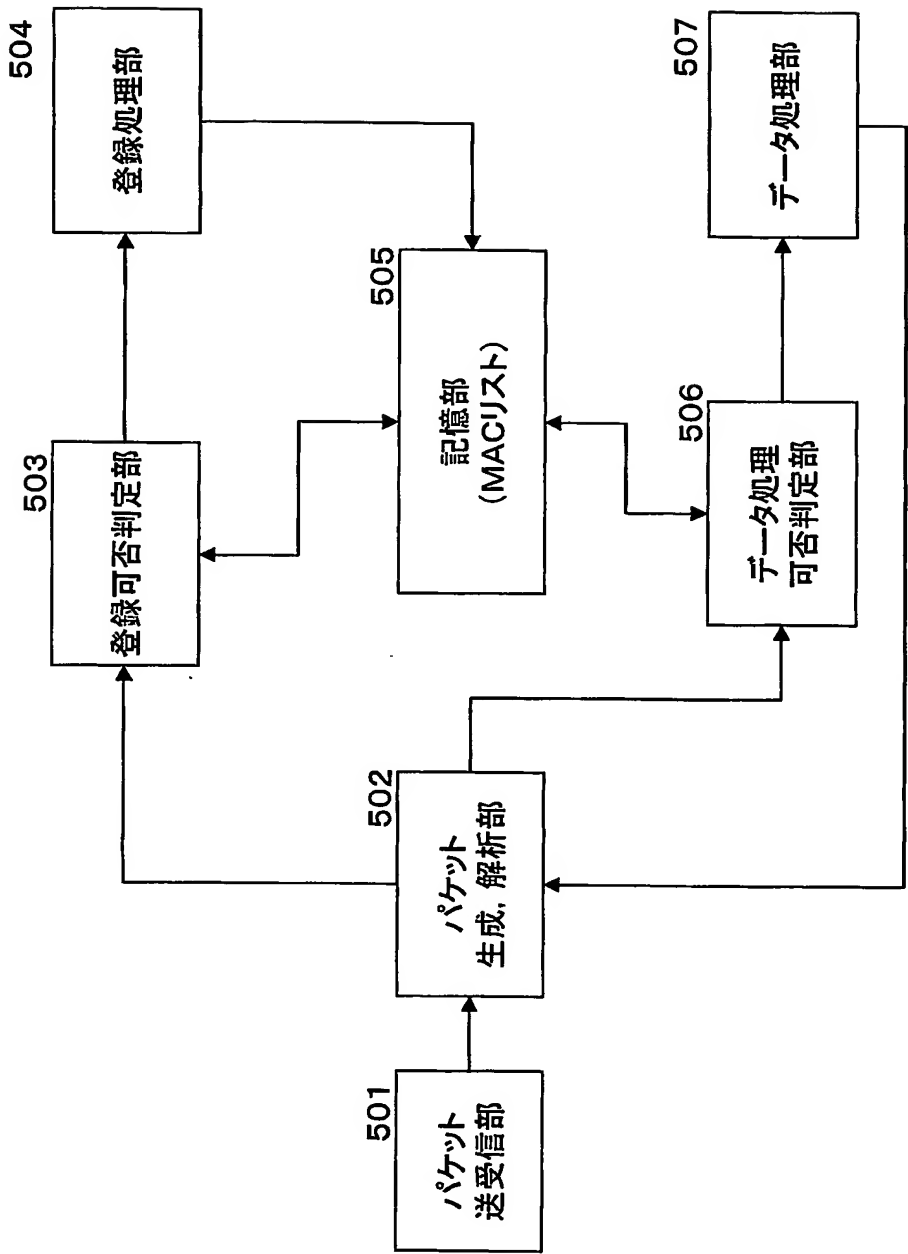


Fig.3

スロットNo.	登録データ.
#01	MACアドレス/クライアント名/登録日時/(ID, キー情報)その他
#02	MACアドレス/クライアント名/登録日時/(ID, キー情報)その他
#03	(空きスロット)
#04	(クロス)
	(クロス)

Fig.4

5/11

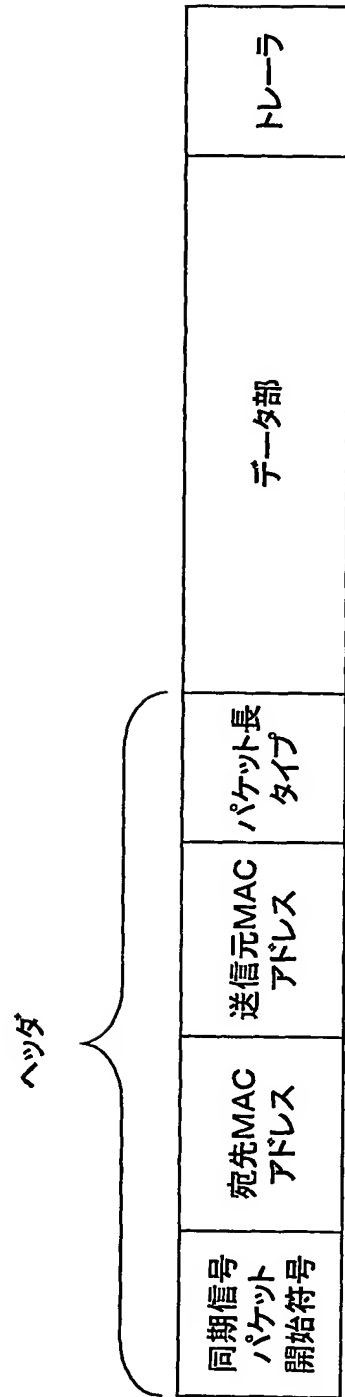
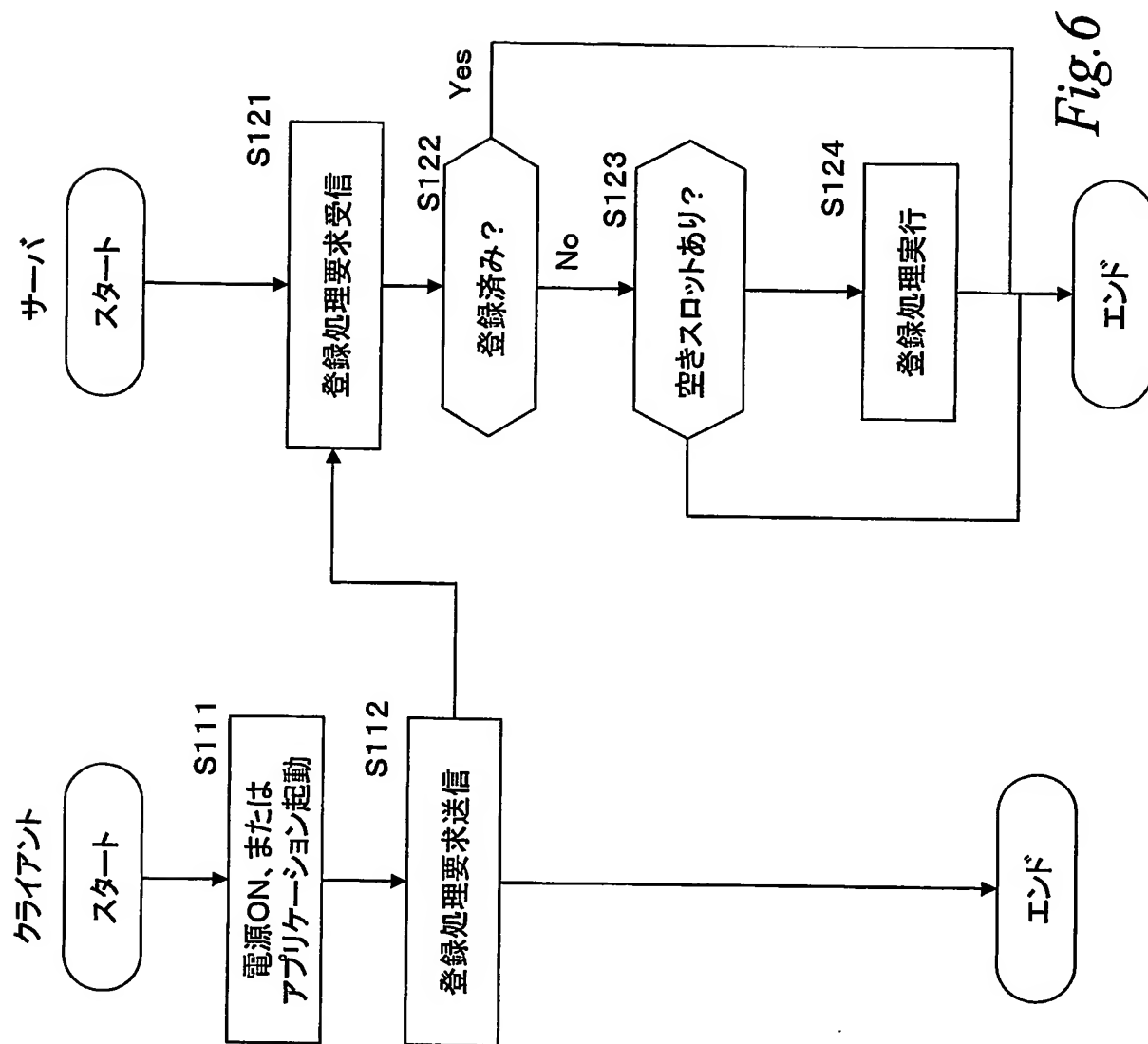


Fig. 5

6/11



7/11

B-POST*HTTP/1.1
HOST:192.254.255.255:3536
Content-Type:application/...
Content-Length:65
Broadcast SNAC
Method:Register

Fig. 7

8/11

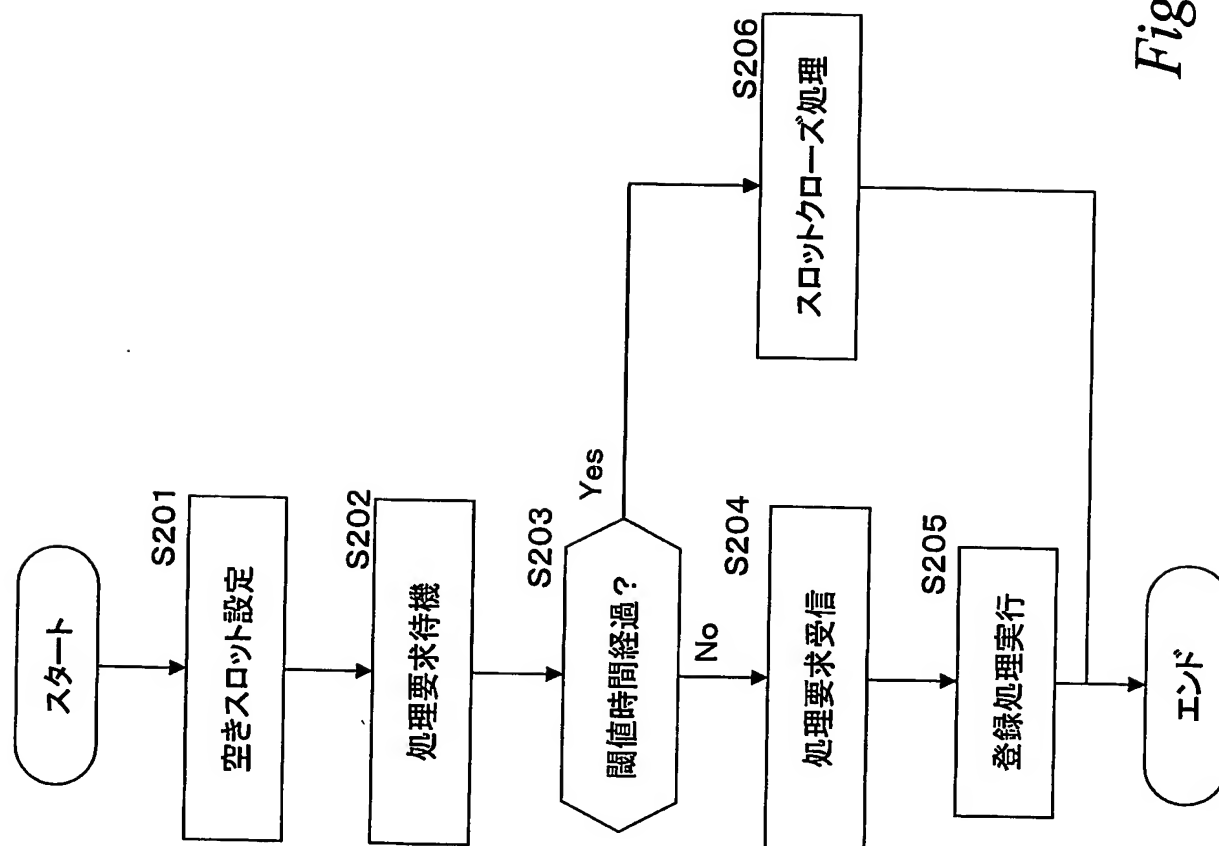
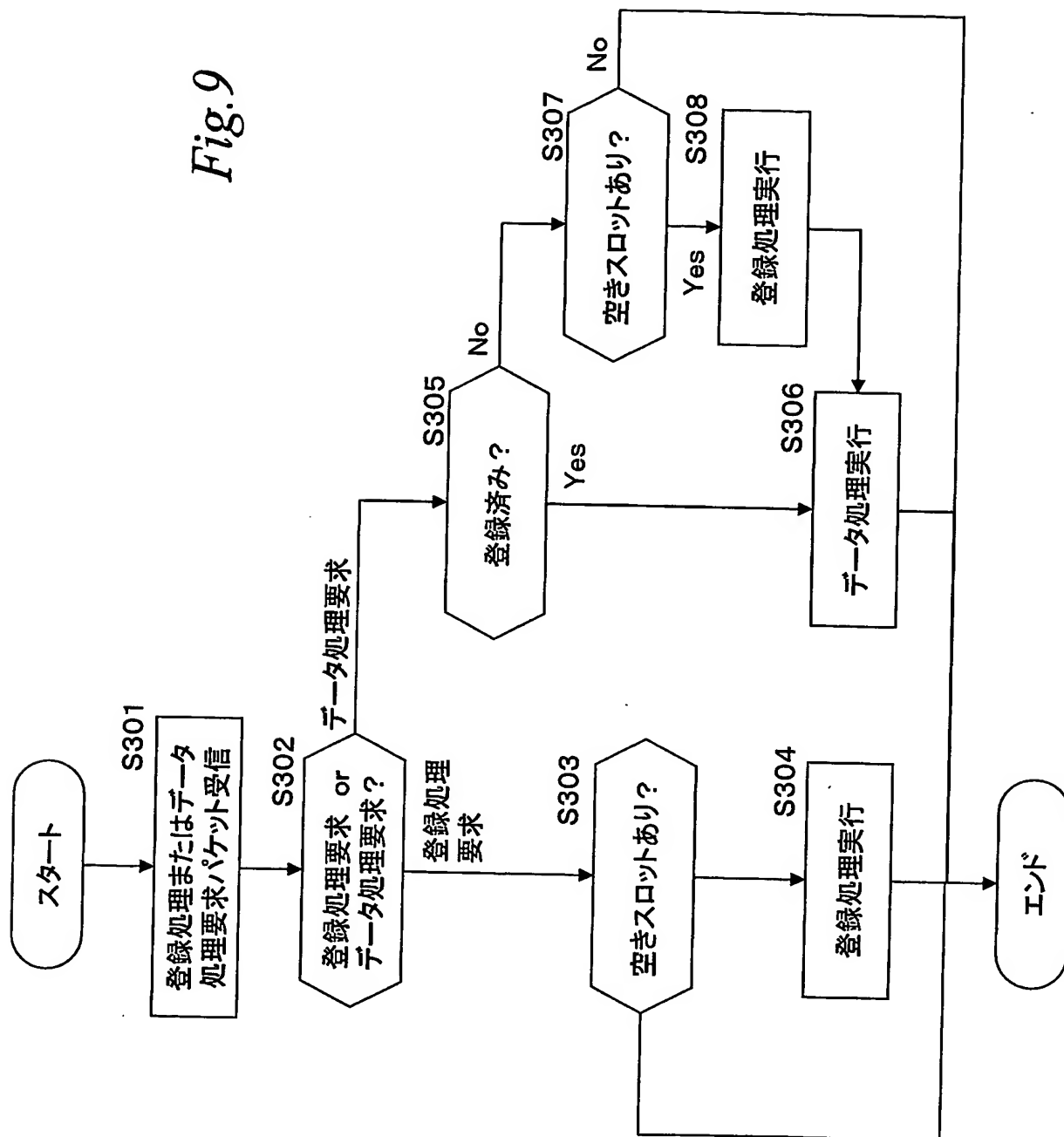


Fig. 8

9/11

Fig.9



10/11

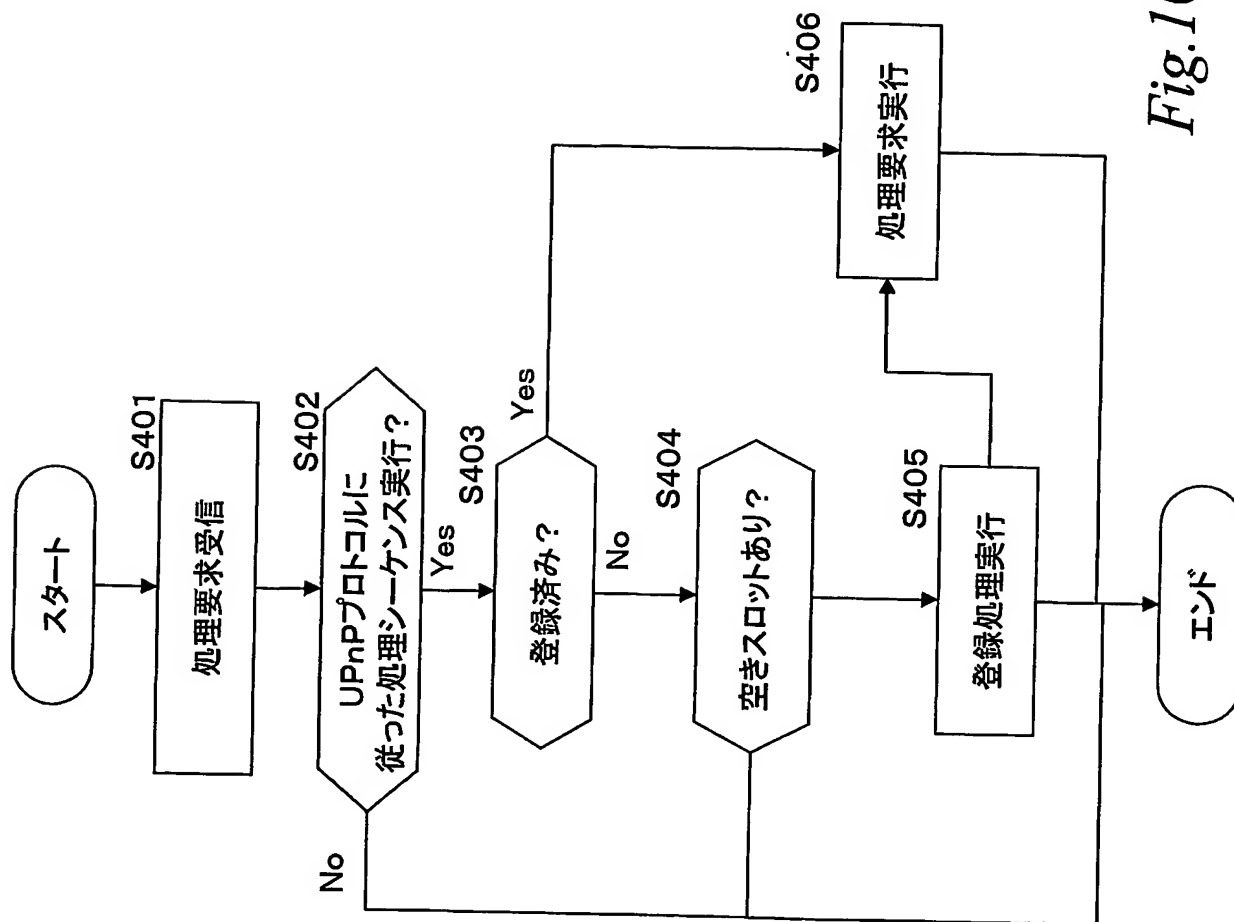


Fig.10

11/11

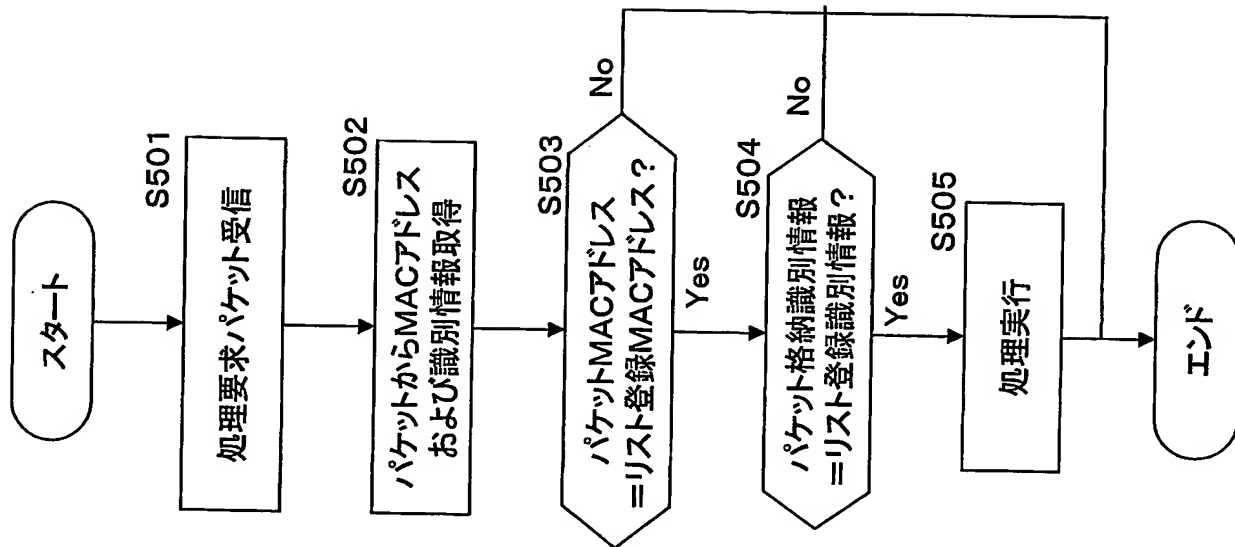


Fig. 11

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/JP03/14634

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L12/28, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L12/28, 44-46

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Toroku Jitsuyo Shinan Koho 1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-159053 A (Toshiba Corp.), 31 May, 2002 (31.05.02),	10-12, 24-26, 28
Y	Full text; Figs. 1 to 34 & US 2002/0061748 A1	1-9, 13-23, 27
Y	JP 9-233111 A (NEC Engineering Kabushiki Kaisha), 05 September, 1997 (05.09.97), Par. No. [0032] (Family: none)	1-9, 13-23, 27
A	JP 2002-325079 A (Matsushita Electric Industrial Co., Ltd.), 08 November, 2002 (08.11.02), Full text; Figs. 1 to 17 & EP 1233538 A2	1-28

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
13 February, 2004 (13.02.04)

Date of mailing of the international search report
24 February, 2004 (24.02.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/14634

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 7-303106 A (NEC Corp.), 14 November, 1995 (14.11.95), Full text; Figs. 1 to 11 (Family: none)	1-28

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L12/28Int. Cl⁷ G06F15/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L12/28, 44-46

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996

日本国公開実用新案公報 1971-2004

日本国実用新案登録公報 1996-2004

日本国登録実用新案公報 1994-2001

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2002-159053 A (株式会社東芝) 2002. 05. 31, 全文, 第1-34図 & US 2002/0061748 A1	10-12, 24-26, 28
Y		1-9, 13-23, 27
Y	JP 9-233111 A (日本電気エンジニアリング株式会社) 1997. 09. 05, 【0032】 (ファミリーなし)	1-9, 13-23, 27

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

13. 02. 2004

国際調査報告の発送日

24. 2. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

宮 島 郁 美

5X

8523

電話番号 03-3581-1101 内線 3595

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2002-325079 A (松下電器産業株式会社) 2002. 11. 08, 全文, 第1-17図 & EP 1233538 A2	1-28
A	JP 7-303106 A (日本電気株式会社) 1995. 11. 14, 全文, 第1-11図 (ファミリーなし)	1-28